3.6.1 – Records Disaster Mitigation and Recovery Plan and Procedures

Standard: There shall be an established records disaster mitigation and recovery plan and procedures that are periodically reviewed for protecting records, storing them, and recovering critical information after a disaster.

Suggested Evidence of Compliance: Provide the records disaster mitigation and recovery plan and procedures and a copy of the most recent review.

The Coral Gables Community Recreation department adheres to the policies and procedures set forth by the Information Technology department when under emergency conditions. The attached IT Departmental Emergency Response Standard Operating Procedures Manual is provided as evidence of compliance. This document was last reviewed and approved by IT director in 2025. The last review date is enclosed as a separate document.

This document goes into detail explaining the process and those involved with the planning of preliminary emergency preparations, maintenance of network and telecommunications, and all recovery post disaster. Also included within the same document is IT's Backup and Recovery Operation Standards which states that the organization requires that all information stored electronically in computerized form be backed up periodically to ensure its safety in the event of a severe hardware interruption, software interruption, virus attack, or other disaster.

In anticipation and preparation of natural disasters, the Community Recreation department has its own internal processes and procedures that should be taken prior to any emergency crisis. Attached you will find the agency's Emergency Management Hurricane Plan which includes a Vital Records Listing for each division in the event facilities cannot be accessed and we are required to work remotely or be relocated. The plan was last updated in May 2025 and presented as part of the annual meeting to Department leadership. See attached meeting agenda, sign-in and presentation.

Security Standards Council®

Payment Card Industry
Data Security Standard

Self-Assessment Questionnaire D for Merchants and Attestation of Compliance

For use with PCI DSS Version 4.0

Revision 1

Publication Date: December 2022

Document Changes

Date	PCI DSS Version	SAQ Revision	Description
October 2008	1.2		To align content with new PCI DSS v1.2 and to implement minor changes noted since original v1.1.
October 2010	2.0		To align content with new PCI DSS v2.0 requirements and testing procedures.
February 2014	3.0		To align content with PCI DSS v3.0 requirements and testing procedures and incorporate additional response options.
April 2015	3.1		Updated to align with PCI DSS v3.1. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.0 to 3.1.
July 2015	3.1	1.1	Updated to remove references to “best practices” prior to June 30, 2015, and remove the PCI DSS v2 reporting option for Requirement 11.3.
April 2016	3.2	1.0	Updated to align with PCI DSS v3.2. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.1 to 3.2.
January 2017	3.2	1.1	Updated version numbering to align with other SAQs.
June 2018	3.2.1	1.0	Updated to align with PCI DSS v3.2.1. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2 to 3.2.1.
April 2022	4.0		Updated to align with PCI DSS v4.0. For details of PCI DSS changes, see PCI DSS – Summary of Changes from PCI DSS Version 3.2.1 to 4.0. Rearranged, retitled, and expanded information in the “Completing the Self-Assessment Questionnaire” section (previously titled “Before You Begin”). Aligned content in Sections 1 and 3 of Attestation of Compliance (AOC) with PCI DSS v4.0 Report on Compliance AOC. Added appendices to support new reporting responses.
December 2022	4.0	1	Removed “In Place with Remediation” as a reporting option from Requirement Responses table, Attestation of Compliance (AOC) Part 2g, SAQ Section 2 Response column, and AOC Section 3. Also removed former Appendix C. Added “In Place with CCW” to AOC Section 3. Added guidance for responding to future-dated requirements. Added minor clarifications and addressed typographical errors.

Contents

Completing the Self-Assessment Questionnaire

Merchant Eligibility Criteria for Self-Assessment Questionnaire D

Self-Assessment Questionnaire (SAQ) D for Merchants applies to merchants that are eligible to complete a self-assessment questionnaire but do not meet the criteria for any other SAQ type. Examples of merchant environments to which SAQ D may apply include but are not limited to:

- E-commerce merchants that accept account data on their website.
- Merchants with electronic storage of account data.
- Merchants that don't store account data electronically but that do not meet the criteria of another SAQ type.
- Merchants with environments that might meet the criteria of another SAQ type, but that have additional PCI DSS requirements applicable to their environment.

This SAQ is not applicable to service providers.

Defining Account Data, Cardholder Data, and Sensitive Authentication Data

PCI DSS is intended for all entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD) or could impact the security of the cardholder data environment (CDE). Cardholder data and sensitive authentication data are considered account data and are defined as follows:

Account Data	
Cardholder Data includes:	**Sensitive Authentication Data includes:**
• Primary Account Number (PAN) • Cardholder Name • Expiration Date • Service Code	• Full track data (magnetic-stripe data or equivalent on a chip) • Card verification code • PINs/PIN blocks

Refer to PCI DSS Section 2, *PCI DSS Applicability Information*, for further details.

PCI DSS Self-Assessment Completion Steps

1. Confirm by review of the eligibility criteria in this SAQ and the *Self-Assessment Questionnaire Instructions and Guidelines* document on PCI SSC website that this is the correct SAQ for the merchant's environment.
2. Confirm that the merchant environment is properly scoped.
3. Assess environment for compliance with PCI DSS requirements.
4. Complete all sections of this document:
   - Section 1: Assessment Information (Parts 1 & 2 of the Attestation of Compliance (AOC) – Contact Information and Executive Summary).
   - Section 2: Self-Assessment Questionnaire D for Merchants.
   - Section 3: Validation and Attestation Details (Parts 3 & 4 of the AOC – PCI DSS Validation and Action Plan for Non-Compliant Requirements (if Part 4 is applicable)).
5. Submit the SAQ and AOC, along with any other requested documentation—such as ASV scan reports—to the requesting organization (those organizations that manage compliance programs such as payment brands and acquirers).

Expected Testing

The instructions provided in the "Expected Testing" column are based on the testing procedures in PCI DSS and provide a high-level description of the types of testing activities that a merchant is expected to perform to verify that a requirement has been met.

The intent behind each testing method is described as follows:

- Examine: The merchant critically evaluates data evidence. Common examples include documents (electronic or physical), screenshots, configuration files, audit logs, and data files.
- Observe: The merchant watches an action or views something in the environment. Examples of observation subjects include personnel performing a task or process, system components performing a function or responding to input, environmental conditions, and physical controls.
- Interview: The merchant converses with individual personnel. Interview objectives may include confirmation of whether an activity is performed, descriptions of how an activity is performed, and whether personnel have particular knowledge or understanding.

The testing methods are intended to allow the merchant to demonstrate how it has met a requirement. The specific items to be examined or observed and personnel to be interviewed should be appropriate for both the requirement being assessed and the merchant's particular implementation.

Full details of testing procedures for each requirement can be found in PCI DSS.

Requirement Responses

For each requirement item, there is a choice of responses to indicate the merchant's status regarding that requirement. ***Only one response should be selected for each requirement item.***

A description of the meaning for each response is provided in the table below:

Response	When to use this response:
In Place	The expected testing has been performed, and all elements of the requirement have been met as stated.
In Place with CCW (Compensating Controls Worksheet)	The expected testing has been performed, and the requirement has been met with the assistance of a compensating control. All responses in this column require completion of a Compensating Controls Worksheet (CCW) in Appendix B of this SAQ. Information on the use of compensating controls and guidance on how to complete the worksheet is provided in PCI DSS Appendices B and C.
Not Applicable	The requirement does not apply to the merchant's environment. (See "Guidance for Not Applicable Requirements" below for examples.) All responses in this column require a supporting explanation in Appendix C of this SAQ.
Not Tested	The requirement was not included for consideration in the assessment and was not tested in any way. (See "Understanding the Difference between Not Applicable and Not Tested" below for examples of when this option should be used.) All responses in this column require a supporting explanation in Appendix D of this SAQ.
Not in Place	Some or all elements of the requirement have not been met, or are in the process of being implemented, or require further testing before the merchant can confirm they are in place. Responses in this column may require the completion of Part 4, if requested by the entity to which this SAQ will be submitted. This response is also used if a requirement cannot be met due to a legal restriction. (See "Legal Exception" below for more guidance).

Guidance for Not Applicable Requirements

While many merchants completing SAQ D will need to validate compliance with every PCI DSS requirement, some entities with very specific business models may find that some requirements do not apply. For example, entities that do not use wireless technology in any capacity are not expected to comply with the PCI DSS requirements that are specific to managing wireless technology. Similarly, entities that do not store any account data electronically at any time are not expected to comply with the PCI DSS requirements related to secure storage of account data (for example, Requirement 3.5.1). Another example is requirements specific to application development and secure coding (for example, Requirements 6.2.1 through 6.2.4), which only apply to an entity with bespoke software (developed for the entity by a third party per the entity's specifications) or custom software (developed by the entity for its own use).

For each response where Not Applicable is selected in this SAQ, complete Appendix C: Explanation of Requirements Noted as Not Applicable.

Understanding the Difference between Not Applicable and Not Tested

Requirements that are deemed to be not applicable to an environment must be verified as such. Using the wireless example above, for a merchant to select "Not Applicable" for Requirements 1.3.3, 2.3.1, 2.3.2, and 4.2.1.2, the merchant first needs to confirm that there are no wireless technologies used in its cardholder data environment (CDE) or that connect to their CDE. Once this has been confirmed, the merchant may select "Not Applicable" for those specific requirements.

If a requirement is completely excluded from review without any consideration as to whether it *could* apply, the "Not Tested" option should be selected. Examples of situations where this could occur may include:

- A merchant is asked by their acquirer to validate a subset of requirements—for example, using the PCI DSS Prioritized Approach to validate only certain milestones.
- A merchant is confirming a new security control that impacts only a subset of requirements—for example, implementation of a new encryption methodology that only requires assessment of PCI DSS Requirements 2, 3, and 4.

In these scenarios, the merchant's assessment only includes certain PCI DSS requirements even though other requirements might also apply to its environment.

If any requirements are completely excluded from the merchant's self-assessment, select Not Tested for that specific requirement, and complete Appendix D: Explanation of Requirements Not Tested for each "Not Tested" entry. An assessment with any Not Tested responses is a "Partial" PCI DSS assessment and will be noted as such by the merchant in the Attestation of Compliance in Section 3, Part 3 of this SAQ.

Guidance for Responding to Future Dated Requirements

In Section 2 below, each new PCI DSS v4.0 requirement or bullet with an extended implementation period includes the following note: "*This requirement [or bullet] is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*"

These new requirements are not required to be included in a PCI DSS assessment until the future date has passed. Prior to that future date, any new requirements with an extended implementation date that have not been implemented by the merchant may be marked as Not Applicable and documented in *Appendix C: Explanation of Requirements Noted as Not Applicable*.

Legal Exception

If your organization is subject to a legal restriction that prevents the organization from meeting a PCI DSS requirement, select Not in Place for that requirement and complete the relevant attestation in Section 3, Part 3 of this SAQ.

Note: *A legal restriction is one where meeting the PCI DSS requirement would violate a local or regional law or regulation.*

Contractual obligations or legal advice are not legal restrictions.

Use of the Customized Approach

Use of the Customized Approach is not supported in SAQs.

SAQs cannot be used to document use of the Customized Approach to meet PCI DSS requirements. For this reason, the Customized Approach Objectives are not included in SAQs. Entities wishing to validate using the Customized Approach may be able to use the PCI DSS Report on Compliance (ROC) Template to document the results of their assessment.

The use of the customized approach may be regulated by organizations that manage compliance programs, such as payment brands and acquirers. Questions about use of a customized approach should always be referred to those organizations. This includes whether an entity that is eligible for an SAQ may instead complete a ROC to use a customized approach, and whether an entity is required to use a QSA, or may use an ISA, to complete an assessment using the customized approach. Information about the use of the Customized Approach can be found in Appendices D and E of PCI DSS.

Additional PCI SSC Resources

Additional resources that provide guidance on PCI DSS requirements and how to complete the self-assessment questionnaire have been provided below to assist with the assessment process.

Resource	Includes:
PCI DSS *(PCI Data Security Standard Requirements and Testing Procedures)*	▪ Guidance on Scoping ▪ Guidance on the intent of all PCI DSS Requirements ▪ Details of testing procedures ▪ Guidance on Compensating Controls ▪ Appendix G: Glossary of Terms, Abbreviations, and Acronyms
SAQ Instructions and Guidelines	▪ Information about all SAQs and their eligibility criteria ▪ How to determine which SAQ is right for your organization
Frequently Asked Questions (FAQs)	▪ Guidance and information about SAQs.
Online PCI DSS Glossary	▪ PCI DSS Terms, Abbreviations, and Acronyms
Information Supplements and Guidelines	▪ Guidance on a variety of PCI DSS topics including: – *Understanding PCI DSS Scoping and Network Segmentation* – *Third-Party Security Assurance* – *Multi-Factor Authentication Guidance* – *Best Practices for Maintaining PCI DSS Compliance*
Getting Started with PCI	▪ Resources for smaller merchants including: – *Guide to Safe Payments* – *Common Payment Systems* – *Questions to Ask Your Vendors* – *Glossary of Payment and Information Security Terms* – *PCI Firewall Basics*

These and other resources can be found on the PCI SSC website *(www.pcisecuritystandards.org)*.

Organizations are encouraged to review PCI DSS and other supporting documents before beginning an assessment.

Section 1: Assessment Information

Instructions for Submission

This document must be completed as a declaration of the results of the merchant's self-assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures.* Complete all sections. The merchant is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which the Attestation of Compliance (AOC) will be submitted for reporting and submission procedures.

Part 1. Contact Information

Part 1a. Assessed Merchant

Company name:	City of Coral Gables
DBA (doing business as):	
Company mailing address:	2801 Salzedo St, FL 33134 , USA
Company main website:	https://www.coralgables.com/
Company contact name:	Raimundo Rodulfo
Company contact title:	Chief Information Officer
Contact phone number:	305-446-6800
Contact e-mail address:	rrodulfo@coralgables.com

Part 1b. Assessor

Provide the following information for all assessors involved in the assessment. If there was no assessor for a given assessor type, enter Not Applicable.

PCI SSC Internal Security Assessor(s)	
ISA name(s):	Not Applicable
Qualified Security Assessor	
Company name:	Enterprise Risk Management d.b.a ERMProtect
Company mailing address:	800 South Douglas Road, Suite 940
Company website:	https://www.ermprotect.com
Lead Assessor Name:	Akash Desai
Assessor phone number:	(305)447-6750
Assessor e-mail address:	adesai@ermprotect.com
Assessor certificate number:	205-788

Part 2. Executive Summary

Part 2a. Merchant Business Payment Channels (select all that apply):

Indicate all payment channels used by the business that are included in this assessment.

☒ Mail order/telephone order (MOTO)

☒ E-Commerce

☒ Card-present

Are any payment channels not included in this assessment?	□ Yes ☒ No
If yes, indicate which channel(s) is not included in the assessment and provide a brief explanation about why the channel was excluded.	Not Applicable

Note: *If the organization has a payment channel that is not covered by this SAQ, consult with the entity(ies) to which this AOC will be submitted about validation for the other channels.*

Part 2b. Description of Role with Payment Cards

For each payment channel included in this assessment as selected in Part 2a above, describe how the business stores, processes, and/or transmits account data.

Channel	How Business Stores, Processes, and/or Transmits Account Data
All Payment Channels	The City is a merchant for several citizen services such as parking payment services and online payments. The City of Coral Gables accepts and processes credit card payments but does NOT store credit cards numbers. Where transmission is applicable, information is securely exchanged using acceptable industry encryption such as TLS 1.2 or IPSec.

Part 2c. Description of Payment Card Environment

Provide a ***high-level*** description of the environment covered by this assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).* • *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.* • *System components that could impact the security of account data.*	The City of Coral Gables is a merchant comprised of payment applications to pay for services online and parking time for users in the City of Coral Gables. Firewall rules are implemented allowing only IP traffic that are required based on the business need. VLANS are used to segment the network logically based on the isolation rules. They don't have wireless deployed in the card holder environment.
Indicate whether the environment includes segmentation to reduce the scope of the assessment. *(Refer to "Segmentation" section of PCI DSS for guidance on segmentation.)*	☒ Yes □ No

Part 2. Executive Summary *(continued)*

Part 2d. In-Scope Locations/Facilities

List all types of physical locations/facilities (for example, retail locations, corporate offices, data centers, call centers, and mail rooms) in scope for the PCI DSS assessment.

Facility Type	**Total number of locations** (How many locations of this type are in scope)	Location(s) of facility (city, country)
Example: Data centers	*3*	*Boston, MA, USA*
Data Center	1	Coral Gables, FL, USA

Part 2e. PCI SSC Validated Products and Solutions

Does the merchant use any item identified on any PCI SSC Lists of Validated Products and Solutions[♦]?

☒ Yes ☐ No

Provide the following information regarding each item the merchant uses from PCI SSC's Lists of Validated Products and Solutions.

Name of PCI SSC-validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which product or solution was validated	PCI SSC listing reference number	Expiry date of listing (YYYY-MM-DD)
T2 Flex and ParkingSoft Evironment	Secure Software Standard v1.2	Secure Software Standard	24-48.00040.001	2025-08-13
Toast	Secure Software Standard v1.2	Secure Software Standard	23-49.01155.001	2025-07-24

[♦] For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components appearing on the PCI SSC website (www.pcisecuritystandards.org)—for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Payment Applications (PA-DSS), Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, and Contactless Payments on COTS (CPoC) solutions.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers

Does the merchant have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the merchant's behalf (for example, payment gateways, payment processors, payment service providers (PSPs), and off-site storage)	☒ Yes ☐ No
• Manage system components included in the scope of the merchant's PCI DSS assessment—for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting services, and IaaS, PaaS, SaaS, and FaaS cloud providers.	☐ Yes ☒ No
• Could impact the security of the merchant's CDE (for example, vendors providing support via remote access, and/or bespoke software developers)	☐ Yes ☒ No

If Yes:

Name of service provider:	Description of service(s) provided:
PayByPhone	Parking Payment provider
WPS	Parking Payment provider
T2	Parking Payment provider
Tyler	Citywide payment gateway
Toast	Country Club Café POS & Payment provider

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment

(SAQ Section 2 and related appendices)

Indicate below all responses that were selected for each PCI DSS requirement.

PCI DSS Requirement	**Requirement Responses** *More than one response may be selected for a given requirement. Indicate all responses that apply.*				
	In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
Requirement 1:	☒	□	☒	□	□
Requirement 2:	☒	□	☒	□	□
Requirement 3:	☒	□	☒	□	□
Requirement 4:	☒	□	☒	□	□
Requirement 5:	☒	□	☒	□	□
Requirement 6:	☒	□	☒	□	□
Requirement 7:	☒	□	☒	□	□
Requirement 8:	☒	□	☒	□	□
Requirement 9:	☒	□	☒	□	□
Requirement 10:	☒	□	☒	□	□
Requirement 11:	☒	□	☒	□	□
Requirement 12:	☒	□	☒	□	□
Appendix A2:	□	□	☒	□	□

Section 2: Self-Assessment Questionnaire D for Merchants

Note: *The following requirements mirror the requirements in the* PCI DSS Requirements and Testing Procedures *document.*

Self-assessment completion date: 2024-10-15

Build and Maintain a Secure Network and Systems

Requirement 1: Install and Maintain Network Security Controls

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.1 Processes and mechanisms for installing and maintaining network security controls are defined and understood.							
1.1.1	All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
1.1.2	Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
1.2 Network security controls (NSCs) are configured and maintained.							
1.2.1	Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	• Examine configurations standards. • Examine configuration settings.	☒	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.2.2	All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	• Examine documented procedures. • Examine network configurations. • Examine change control records. • Interview responsible personnel.	☒	☐	☐	☐	☐
	Applicability Notes						
	Changes to network connections include the addition, removal, or modification of a connection. Changes to NSC configurations include those related to the component itself as well as those affecting how it performs its security function.						
1.2.3	An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	• Examine network diagrams. • Examine network configurations. • Interview responsible personnel.	☒	☐	☐	☐	☐
	Applicability Notes						
	A current network diagram(s) or other technical or topological solution that identifies network connections and devices can be used to meet this requirement.						
1.2.4	An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	• Examine data flow diagrams. • Observe network configurations. • Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
	Applicability Notes						
	A data-flow diagram(s) or other technical or topological solution that identifies flows of account data across systems and networks can be used to meet this requirement.						
1.2.5	All services, protocols and ports allowed are identified, approved, and have a defined business need.	• Examine documentation. • Examine configuration settings.	☒	☐	☐	☐	☐
1.2.6	Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	• Examine documentation. • Examine configuration settings.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.2.7	Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	• Examine documented procedures. • Examine documentation from reviews performed. • Examine configuration settings.	☒	☐	☐	☐	☐
1.2.8	Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	• Examine NSC configuration files.	☒	☐	☐	☐	☐
	Applicability Notes						
	Any file or setting used to configure or synchronize NSCs is considered to be a “configuration file.” This includes files, automated and system-based controls, scripts, settings, infrastructure as code, or other parameters that are backed up, archived, or stored remotely.						
1.3 Network access to and from the cardholder data environment is restricted.							
1.3.1	Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary, • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☒	☐	☐	☐	☐
1.3.2	Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	• Examine NSC configuration standards. • Examine NSC configurations.	☒	☐	☐	☐	☐
1.3.3	NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	• Examine configuration settings. • Examine network diagrams.	☐	☐	☒	☐	☐
1.4 Network connections between trusted and untrusted networks are controlled.							
1.4.1	NSCs are implemented between trusted and untrusted networks.	• Examine NSC configuration standards. • Examine current network diagrams. • Examine network configurations.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	**Response♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.4.2	Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	• Examine NSC documentation. • Examine NSC configurations.	☒	☐	☐	☐	☐
	Applicability Notes						
	The intent of this requirement is to address communication sessions between trusted and untrusted networks, rather than the specifics of protocols. This requirement does not limit the use of UDP or other connectionless network protocols if state is maintained by the NSC.						
1.4.3	Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	• Examine NSC documentation. • Examine NSC configurations.	☒	☐	☐	☐	☐
1.4.4	System components that store cardholder data are not directly accessible from untrusted networks.	• Examine the data-flow diagram and network diagram. • Examine NSC configurations.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is not intended to apply to storage of account data in volatile memory but does apply where memory is being treated as persistent storage (for example, RAM disk). Account data can only be stored in volatile memory during the time necessary to support the associated business process (for example, until completion of the related payment card transaction).						
1.4.5	The disclosure of internal IP addresses and routing information is limited to only authorized parties.	• Examine NSC configurations. • Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
1.5 Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.							
1.5.1	Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows. • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	• Examine policies and configuration standards. • Examine device configuration settings.	☒	☐	☐	☐	☐
	Applicability Notes						
	These security controls may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If these security controls need to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which these security controls are not active. This requirement applies to employee-owned and company-owned computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit.						

Requirement 2: Apply Secure Configurations to All System Components

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.							
2.1.1	All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
2.1.2	Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
2.2 System components are configured and managed securely.							
2.2.1	Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	• Examine system configuration standards. • Review industry-accepted hardening standards. • Examine configuration settings. • Interview personnel.	☒	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
2.2.2	Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	• Examine system configuration standards. • Examine vendor documentation. • Observe a system administrator logging on using vendor default accounts. • Examine configuration files. • Interview personnel.	☒	☐	☐	☐	☐
	Applicability Notes						
	This applies to ALL vendor default accounts and passwords, including, but not limited to, those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment applications, and Simple Network Management Protocol (SNMP) defaults. This requirement also applies where a system component is not installed within an entity's environment, for example, software and applications that are part of the CDE and are accessed via a cloud subscription service.						
2.2.3	Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from each other, **OR** • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	• Examine system configuration standards. • Examine system configurations.	☒	☐	☐	☐	☐
2.2.4	Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	• Examine system configuration standards. • Examine system configurations.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
2.2.5	If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	• Examine configuration standards. • Interview personnel. • Examine configuration settings.	□	□	☒	□	□
2.2.6	System security parameters are configured to prevent misuse.	• Examine system configuration standards. • Interview personnel. • Examine system configurations.	☒	□	□	□	□
2.2.7	All non-console administrative access is encrypted using strong cryptography.	• Examine system configuration standards. • Observe an administrator log on. • Examine system configurations. • Examine vendor documentation. • Interview personnel.	☒	□	□	□	□
	Applicability Notes						
	This includes administrative access via browser-based interfaces and application programming interfaces (APIs).						

PCI DSS Requirement		Expected Testing	**Response♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
2.3 Wireless environments are configured and managed securely.							
2.3.1	For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults. • Any other security-related wireless vendor defaults.	• Examine policies and procedures. • Review vendor documentation. • Examine wireless configuration settings. • Interview personnel.	□	□	☒	□	□
	Applicability Notes						
	This includes, but is not limited to, default wireless encryption keys, passwords on wireless access points, SNMP defaults, and any other security-related wireless vendor defaults.						
2.3.2	For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	• Examine key-management documentation. • Interview personnel.	□	□	☒	□	□

Protect Account Data

Requirement 3: Protect Stored Account Data

PCI DSS Requirement		Expected Testing	Response [♦] *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.1 Processes and mechanisms for protecting stored account data are defined and understood.							
3.1.1	All security policies and operational procedures that are identified in Requirement 3 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
3.1.2	Roles and responsibilities for performing activities in Requirement 3 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	□	□	□	□

[♦] *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.2 Storage of account data is kept to a minimum.							
3.2.1	Account data storage is kept to a minimum through implementation of data retention and disposal policies, procedures, and processes that include at least the following: • Coverage for all locations of stored account data. • Coverage for any sensitive authentication data (SAD) stored prior to completion of authorization. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Limiting data storage amount and retention time to that which is required for legal or regulatory, and/or business requirements. • Specific retention requirements for stored account data that defines length of retention period and includes a documented business justification. • Processes for secure deletion or rendering account data unrecoverable when no longer needed per the retention policy. • A process for verifying, at least once every three months, that stored account data exceeding the defined retention period has been securely deleted or rendered unrecoverable.	• Examine the data retention and disposal policies, procedures, and processes. • Interview personnel. • Examine files and system records on system components where account data is stored. • Observe the mechanisms used to render account data unrecoverable.	☐	☐	☒	☐	☐
	Applicability Notes						
	Where account data is stored by a TPSP (for example, in a cloud environment), entities are responsible for working with their service providers to understand how the TPSP meets this requirement for the entity. Considerations include ensuring that all geographic instances of a data element are securely deleted. *The bullet above (for coverage of SAD stored prior to completion of authorization) is a best practice until 31 March 2025, after which it will be required as part of Requirement 3.2.1 and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.3 Sensitive authentication data (SAD) is not stored after authorization.							
3.3.1	SAD is not retained after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.	• Examine documented policies and procedures. • Examine system configurations. • Observe the secure data deletion processes.	☐	☐	☒	☐	☐
	Applicability Notes						
	Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments. Sensitive authentication data includes the data cited in Requirements 3.3.1.1 through 3.3.1.3.						
3.3.1.1	The full contents of any track are not retained upon completion of the authorization process.	• Examine data sources.	☐	☐	☒	☐	☐
	Applicability Notes						
	In the normal course of business, the following data elements from the track may need to be retained: • Cardholder name. • Primary account number (PAN). • Expiration date. • Service code. To minimize risk, store securely only these data elements as needed for business.						
3.3.1.2	The card verification code is not retained upon completion of the authorization process.	• Examine data sources.	☐	☐	☒	☐	☐
	Applicability Notes						
	The card verification code is the three- or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions.						
3.3.1.3	The personal identification number (PIN) and the PIN block are not retained upon completion of the authorization process.	• Examine data sources.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Applicability Notes PIN blocks are encrypted during the natural course of transaction processes, but even if an entity encrypts the PIN block again, it is still not allowed to be stored after the completion of the authorization process.						
3.3.2	SAD that is stored electronically prior to completion of authorization is encrypted using strong cryptography.	• Examine data stores and system configurations. • Examine vendor documentation.	□	□	☒	□	□
	Applicability Notes Whether SAD is permitted to be stored prior to authorization is determined by the organizations that manage compliance programs (for example, payment brands and acquirers). Contact the organizations of interest for any additional criteria. This requirement applies to all storage of SAD, even if no PAN is present in the environment. Refer to Requirement 3.2.1 for an additional requirement that applies if SAD is stored prior to completion of authorization. *Part of this Applicability Note was intentionally removed for this SAQ as it does not apply to merchant assessments*. This requirement does not replace how PIN blocks are required to be managed, nor does it mean that a properly encrypted PIN block needs to be encrypted again. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
3.3.3	***Additional requirement for service providers only***						

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.4 Access to displays of full PAN and ability to copy PAN is restricted.							
3.4.1	PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.	• Examine documented policies and procedures. • Examine system configurations. • Examine the documented list of roles that need access to more than the BIN and last four digits of the PAN (includes full PAN). • Examine displays of PAN (for example, on screen, on paper receipts).	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment brand requirements for point-of-sale (POS) receipts. This requirement relates to protection of PAN where it is displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.5.1 for protection of PAN when stored, processed, or transmitted.						
3.4.2	When using remote-access technologies, technical controls prevent copy and/or relocation of PAN for all personnel, except for those with documented, explicit authorization and a legitimate, defined business need.	• Examine documented policies and procedures and documented evidence for technical controls. • Examine configurations for remote-access technologies. • Observe processes. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	Storing or relocating PAN onto local hard drives, removable electronic media, and other storage devices brings these devices into scope for PCI DSS. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response♦ (*Check one response for each requirement*)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.5 Primary account number (PAN) is secured wherever it is stored.							
3.5.1	PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). – If hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place such that the different versions cannot be correlated to reconstruct the original PAN • Index tokens. • Strong cryptography with associated key-management processes and procedures.	• Examine documentation about the system used to render PAN unreadable. • Examine data repositories. • Examine audit logs, including payment application logs. • Examine controls to verify that the hashed and truncated PANs cannot be correlated to reconstruct the original PAN.	☐	☐	☒	☐	☐
	Applicability Notes						
	It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN						
3.5.1.1	Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7.	• Examine documentation about the hashing method used. • Examine documentation about the key-management procedures and processes. • Examine data repositories. • Examine audit logs, including payment application logs.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Applicability Notes This requirement applies to PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception, or troubleshooting logs) must all be protected. This requirement does not preclude the use of temporary files containing cleartext PAN while encrypting and decrypting PAN. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
3.5.1.2	If disk-level or partition-level encryption (rather than file-, column-, or field-level database encryption) is used to render PAN unreadable, it is implemented only as follows: • On removable electronic media. **OR** • If used for non-removable electronic media, PAN is also rendered unreadable via another mechanism that meets Requirement 3.5.1.	• Observe encryption processes. • Examine configurations and/or vendor documentation. • Observe encryption processes.	□	□	☒	□	□
	Applicability Notes While disk encryption may still be present on these types of devices, it cannot be the only mechanism used to protect PAN stored on those systems. Any stored PAN must also be rendered unreadable per Requirement 3.5.1—for example, through truncation or a data-level encryption mechanism. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore its use is appropriate only for removable electronic media storage devices. Media that is part of a data center architecture (for example, hot-swappable drives, bulk tape-backups) is considered non-removable electronic media to which Requirement 3.5.1 applies. Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.5.1.3	If disk-level or partition-level encryption is used (rather than file-, column-, or field--level database encryption) to render PAN unreadable, it is managed as follows: • Logical access is managed separately and independently of native operating system authentication and access control mechanisms. • Decryption keys are not associated with user accounts. • Authentication factors (passwords, passphrases, or cryptographic keys) that allow access to unencrypted data are stored securely.	• Examine system configurations. • Observe the authentication process. • Examine files containing authentication factors. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes Disk or partition encryption implementations must also meet all other PCI DSS encryption and key-management requirements.						

	PCI DSS Requirement	Expected Testing	**Response♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.6 Cryptographic keys used to protect stored account data are secured.							
3.6.1	Procedures are defined and implemented to protect cryptographic keys used to protect stored account data against disclosure and misuse that include: • Access to keys is restricted to the fewest number of custodians necessary. • Key-encrypting keys are at least as strong as the data-encrypting keys they protect. • Key-encrypting keys are stored separately from data-encrypting keys. • Keys are stored securely in the fewest possible locations and forms.	• Examine documented key-management policies and procedures.	□	□	☒	□	□
	Applicability Notes This requirement applies to keys used to encrypt stored account data and to key-encrypting keys used to protect data-encrypting keys. The requirement to protect keys used to protect stored account data from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.						
3.6.1.1	***Additional requirement for service providers only***						

PCI DSS Requirement		Expected Testing	Response♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.6.1.2	Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.	• Examine documented procedures. • Examine system configurations and key storage locations, including for key-encrypting keys.	☐	☐	☒	☐	☐
	Applicability Notes It is not required that public keys be stored in one of these forms. Cryptographic keys stored as part of a key-management system (KMS) that employs SCDs are acceptable. A cryptographic key that is split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within an SCD, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.						
3.6.1.3	Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.	• Examine user access lists.	☐	☐	☒	☐	☐
3.6.1.4	Cryptographic keys are stored in the fewest possible locations.	• Examine key storage locations. • Observe processes.	☐	☐	☒	☐	☐
3.7 Where cryptography is used to protect stored account data, key-management processes and procedures covering all aspects of the key lifecycle are defined and implemented.							
3.7.1	Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for generating keys.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
3.7.2	Key-management policies and procedures are implemented to include secure distribution of cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for distributing keys.	□	□	☒	□	□
3.7.3	Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	• Examine documented key-management policies and procedures. • Observe the method for storing keys.	□	□	☒	□	□
3.7.4	Key-management policies and procedures are implemented for cryptographic key changes for keys that have reached the end of their cryptoperiod, as defined by the associated application vendor or key owner, and based on industry best practices and guidelines, including the following: • A defined cryptoperiod for each key type in use. • A process for key changes at the end of the defined cryptoperiod.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe key storage locations.	□	□	☒	□	□
3.7.5	Key-management policies procedures are implemented to include the retirement, replacement, or destruction of keys used to protect stored account data, as deemed necessary when: • The key has reached the end of its defined cryptoperiod. • The integrity of the key has been weakened, including when personnel with knowledge of a cleartext key component leaves the company, or the role for which the key component was known. • The key is suspected of or known to be compromised. Retired or replaced keys are not used for encryption operations.	• Examine documented key-management policies and procedures. • Interview personnel.	□	□	☒	□	□
	Applicability Notes						

	PCI DSS Requirement	Expected Testing	Response♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key).						
3.7.6	Where manual cleartext cryptographic key-management operations are performed by personnel, key-management policies and procedures are implemented include managing these operations using split knowledge and dual control.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe processes.	☐	☐	☒	☐	☐
	Applicability Notes						
	This control is applicable for manual key-management operations or where key management is not controlled by the encryption product. A cryptographic key that is simply split into two parts does not meet this requirement. Secret or private keys stored as key components or key shares must be generated via one of the following: • Using an approved random number generator and within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device, **OR** • According to ISO 19592 or equivalent industry standard for generation of secret key shares.						
3.7.7	Key-management policies and procedures are implemented to include the prevention of unauthorized substitution of cryptographic keys.	• Examine documented key-management policies and procedures. • Interview personnel. • Observe processes.	☐	☐	☒	☐	☐
3.7.8	Key-management policies and procedures are implemented to include that cryptographic key custodians formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	• Examine documented key-management policies and procedures. • Review documentation or other evidence of key custodian acknowledgments.	☐	☐	☒	☐	☐
3.7.9	***Additional requirement for service providers only***						

Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks

PCI DSS Requirement		Expected Testing	Response[♦] (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
4.1 Processes and mechanisms for protecting cardholder data with strong cryptography during transmission over open, public networks are defined and documented.							
4.1.1	All security policies and operational procedures that are identified in Requirement 4 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
4.1.2	Roles and responsibilities for performing activities in Requirement 4 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel	☒	□	□	□	□

[♦] *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
4.2 PAN is protected with strong cryptography during transmission.							
4.2.1	Strong cryptography and security protocols are implemented as follows to safeguard PAN during transmission over open, public networks:						
	• Only trusted keys and certificates are accepted.	• Examine documented policies and procedures. • Interview personnel. • Examine system configurations. • Examine cardholder data transmissions. • Examine keys and certificates.	☒	☐	☐	☐	☐
	• Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.*		☐	☐	☒	☐	☐
	• The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations.		☒	☐	☐	☐	☐
	• The encryption strength is appropriate for the encryption methodology in use.		☒	☐	☐	☐	☐
	Applicability Notes						
	There could be occurrences where an entity receives cardholder data unsolicited via an insecure communication channel that was not intended for the purpose of receiving sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or implement measures to prevent the channel from being used for cardholder data. A self-signed certificate may also be acceptable if the certificate is issued by an internal CA within the organization, the certificate's author is confirmed, and the certificate is verified—for example, via hash or signature—and has not expired. Note that self-signed certificates where the Distinguished Name (DN) field in the "issued by" and "issued to" field is the same are not acceptable. *The bullet above (for confirming that certificates used to safeguard PAN during transmission over open, public networks are valid and are not expired or revoked) is a best practice until 31 March 2025, after which it will be required as part of Requirement 4.2.1 and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	**Response♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
4.2.1.1	An inventory of the entity's trusted keys and certificates used to protect PAN during transmission is maintained.	• Examine documented policies and procedures. • Examine the inventory of trusted keys and certificates.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
4.2.1.2	Wireless networks transmitting PAN or connected to the CDE use industry best practices to implement strong cryptography for authentication and transmission.	• Examine system configurations.	☐	☐	☒	☐	☐
4.2.2	PAN is secured with strong cryptography whenever it is sent via end-user messaging technologies.	• Examine documented policies and procedures. • Examine system configurations and vendor documentation.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement also applies if a customer, or other third-party, requests that PAN is sent to them via end-user messaging technologies. There could be occurrences where an entity receives unsolicited cardholder data via an insecure communication channel that was not intended for transmissions of sensitive data. In this situation, the entity can choose to either include the channel in the scope of their CDE and secure it according to PCI DSS or delete the cardholder data and implement measures to prevent the channel from being used for cardholder data.						

Maintain a Vulnerability Management Program

Requirement 5: Protect All Systems and Networks from Malicious Software

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
5.1 Processes and mechanisms for protecting all systems and networks from malicious software are defined and understood.							
5.1.1	All security policies and operational procedures that are identified in Requirement 5 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
5.1.2	Roles and responsibilities for performing activities in Requirement 5 are documented, assigned, and understood. New requirement - effective immediately	• Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
5.2 Malicious software (malware) is prevented, or detected and addressed.							
5.2.1	An anti-malware solution(s) is deployed on all system components, except for those system components identified in periodic evaluations per Requirement 5.2.3 that concludes the system components are not at risk from malware.	• Examine system components. • Examine the periodic evaluations.	☒	☐	☐	☐	☐
5.2.2	The deployed anti-malware solution(s): • Detects all known types of malware. • Removes, blocks, or contains all known types of malware.	• Examine vendor documentation. • Examine system configurations.	☒	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

	PCI DSS Requirement	Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
5.2.3	Any system components that are not at risk for malware are evaluated periodically to include the following: • A documented list of all system components not at risk for malware. • Identification and evaluation of evolving malware threats for those system components. • Confirmation whether such system components continue to not require anti-malware protection.	• Examine documented policies and procedures. • Interview personnel. • Examine the list of system components not at risk for malware and compare against the system components without an anti-malware solution deployed.	☐	☐	☒	☐	☐
	Applicability Notes						
	System components covered by this requirement are those for which there is no anti-malware solution deployed per Requirement 5.2.1.						
5.2.3.1	The frequency of periodic evaluations of system components identified as not at risk for malware is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	• Examine the targeted risk analysis. • Examine documented results of periodic evaluations. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3 Anti-malware mechanisms and processes are active, maintained, and monitored.							
5.3.1	The anti-malware solution(s) is kept current via automatic updates.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components and logs.	☒	☐	☐	☐	☐
5.3.2	The anti-malware solution(s): • Performs periodic scans and active or real-time scans OR • Performs continuous behavioral analysis of systems or processes.	• Examine anti-malware solution(s) configurations, including any master installation. • Examine system components. • Examine logs and scan results.	☒	☐	☐	☐	☐

PCI DSS Requirement		**Expected Testing**	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
5.3.2.1	If periodic malware scans are performed to meet Requirement 5.3.2, the frequency of scans is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	• Examine the targeted risk analysis. • Examine documented results of periodic malware scans. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement applies to entities conducting periodic malware scans to meet Requirement 5.3.2. This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3.3	For removable electronic media, the anti-malware solution(s): • Performs automatic scans of when the media is inserted, connected, or logically mounted, **OR** • Performs continuous behavioral analysis of systems or processes when the media is inserted, connected, or logically mounted.	• Examine anti-malware solution(s) configurations. • Examine system components with removable electronic media. • Examine logs and scan results.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
5.3.4	Audit logs for the anti-malware solution(s) are enabled and retained in accordance with Requirement 10.5.1.	• Examine anti-malware solution(s) configurations.	☒	☐	☐	☐	☐
5.3.5	Anti-malware mechanisms cannot be disabled or altered by users, unless specifically documented, and authorized by management on a case-by-case basis for a limited time period.	• Examine anti-malware configurations. • Observe processes. • Interview responsible personnel.	☒	☐	☐	☐	☐
	Applicability Notes *(Continued)*						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Anti-malware solutions may be temporarily disabled only if there is a legitimate technical need, as authorized by management on a case-by-case basis. If anti-malware protection needs to be disabled for a specific purpose, it must be formally authorized. Additional security measures may also need to be implemented for the period during which anti-malware protection is not active.						
5.4 Anti-phishing mechanisms protect users against phishing attacks.							
5.4.1	Processes and automated mechanisms are in place to detect and protect personnel against phishing attacks.	• Observe implemented processes. • Examine mechanisms.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement applies to the automated mechanism. It is not intended that the systems and services providing such automated mechanisms (such as e-mail servers) are brought into scope for PCI DSS. The focus of this requirement is on protecting personnel with access to system components in-scope for PCI DSS. Meeting this requirement for technical and automated controls to detect and protect personnel against phishing is not the same as Requirement 12.6.3.1 for security awareness training. Meeting this requirement does not also meet the requirement for providing personnel with security awareness training, and vice versa. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

Requirement 6: Develop and Maintain Secure Systems and Software

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.1 Processes and mechanisms for developing and maintaining secure systems and software are defined and understood.							
6.1.1	All security policies and operational procedures that are identified in Requirement 6 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
6.1.2	Roles and responsibilities for performing activities in Requirement 6 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	□	□	□	□
6.2 Bespoke and custom software are developed securely.							
6.2.1	Bespoke and custom software are developed securely, as follows: • Based on industry standards and/or best practices for secure development. • In accordance with PCI DSS (for example, secure authentication and logging). • Incorporating consideration of information security issues during each stage of the software development lifecycle.	• Examine documented software development procedures.	□	□	☒	□	□
	Applicability Notes						
	This applies to all software developed for or by the entity for the entity's own use. This includes both bespoke and custom software. This does not apply to third-party software.						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.2.2	Software development personnel working on bespoke and custom software are trained at least once every 12 months as follows: • On software security relevant to their job function and development languages. • Including secure software design and secure coding techniques. • Including, if security testing tools are used, how to use the tools for detecting vulnerabilities in software.	• Examine documented software development procedures. • Examine training records. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	Software development personnel remain knowledgeable about secure development practices; software security; and attacks against the languages, frameworks, or applications they develop. Personnel are able to access assistance and guidance when required.						
6.2.3	Bespoke and custom software is reviewed prior to being released into production or to customers, to identify and correct potential coding vulnerabilities, as follows: • Code reviews ensure code is developed according to secure coding guidelines. • Code reviews look for both existing and emerging software vulnerabilities. • Appropriate corrections are implemented prior to release.	• Examine documented software development procedures. • Interview responsible personnel. • Examine evidence of changes to bespoke and custom software.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement for code reviews applies to all bespoke and custom software (both internal and public-facing), as part of the system development lifecycle. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.4. Code reviews may be performed using either manual or automated processes, or a combination of both.						

	PCI DSS Requirement	Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.2.3.1	If manual code reviews are performed for bespoke and custom software prior to release to production, code changes are: • Reviewed by individuals other than the originating code author, and who are knowledgeable about code-review techniques and secure coding practices. • Reviewed and approved by management prior to release.	• Examine documented software development procedures. • Interview responsible personnel. • Examine evidence of changes to bespoke and custom software.	☐	☐	☒	☐	☐
	Applicability Notes						
	Manual code reviews can be conducted by knowledgeable internal personnel or knowledgeable third-party personnel. An individual that has been formally granted accountability for release control and who is neither the original code author nor the code reviewer fulfills the criteria of being management.						
6.2.4	Software engineering techniques or other methods are defined and in use by software development personnel to prevent or mitigate common software attacks and related vulnerabilities in bespoke and custom software, including but not limited to the following:						
	• Injection attacks, including SQL, LDAP, XPath, or other command, parameter, object, fault, or injection-type flaws.	• Examine documented procedures. • Interview responsible software development personnel.	☐	☐	☒	☐	☐
	• Attacks on data and data structures, including attempts to manipulate buffers, pointers, input data, or shared data.		☐	☐	☒	☐	☐
	• Attacks on cryptography usage, including attempts to exploit weak, insecure, or inappropriate cryptographic implementations, algorithms, cipher suites, or modes of operation.		☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.2.4 *(cont.)*	• Attacks on business logic, including attempts to abuse or bypass application features and functionalities through the manipulation of APIs, communication protocols and channels, client-side functionality, or other system/application functions and resources. This includes cross-site scripting (XSS) and cross-site request forgery (CSRF). *(continued)*		☐	☐	☒	☐	☐
	• Attacks on access control mechanisms, including attempts to bypass or abuse identification, authentication, or authorization mechanisms, or attempts to exploit weaknesses in the implementation of such mechanisms.		☐	☐	☒	☐	☐
	• Attacks via any “high-risk” vulnerabilities identified in the vulnerability identification process, as defined in Requirement 6.3.1.		☐	☐	☒	☐	☐
	Applicability Notes						
	This applies to all software developed for or by the entity for the entity’s own use. This includes both bespoke and custom software. This does not apply to third-party software.						
6.3 Security vulnerabilities are identified and addressed.							
6.3.1	Security vulnerabilities are identified and managed as follows: • New security vulnerabilities are identified using industry-recognized sources for security vulnerability information, including alerts from international and national computer emergency response teams (CERTs). • Vulnerabilities are assigned a risk ranking based on industry best practices and consideration of potential impact. • Risk rankings identify, at a minimum, all vulnerabilities considered to be a high-risk or critical to the environment. • Vulnerabilities for bespoke and custom, and third-party software (for example operating systems and databases) are covered.	• Examine policies and procedures. • Interview responsible personnel. • Examine documentation. • Observe processes.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Applicability Notes *(Continued)*						
	This requirement is not achieved by, nor is it the same as, vulnerability scans performed for Requirements 11.3.1 and 11.3.2. This requirement is for a process to actively monitor industry sources for vulnerability information and for the entity to determine the risk ranking to be associated with each vulnerability.						
6.3.2	An inventory of bespoke and custom software, and third-party software components incorporated into bespoke and custom software is maintained to facilitate vulnerability and patch management.	• Examine documentation. • Interview personnel. •	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment						
6.3.3	All system components are protected from known vulnerabilities by installing applicable security patches/updates as follows: • Critical or high-security patches/updates (identified according to the risk ranking process at Requirement 6.3.1) are installed within one month of release. • All other applicable security patches/updates are installed within an appropriate time frame as determined by the entity (for example, within three months of release).	• Examine policies and procedures. • Examine system components and related software. • Compare list of security patches installed to recent vendor patch lists.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.4 Public-facing web applications are protected against attacks.							
6.4.1	For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis and these applications are protected against known attacks as follows: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods as follows: – At least once every 12 months and after significant changes. – By an entity that specializes in application security. – Including, at a minimum, all common software attacks in Requirement 6.2.4. – All vulnerabilities are ranked in accordance with Requirement 6.3.1. – All vulnerabilities are corrected. – The application is re-evaluated after the corrections **OR** • Installing an automated technical solution(s) that continually detects and prevents web-based attacks as follows: – Installed in front of public-facing web applications to detect and prevent web-based attacks. – Actively running and up to date as applicable. – Generating audit logs. – Configured to either block web-based attacks or generate an alert that is immediately investigated.	• Examine documented processes. • Interview personnel. • Examine records of application security assessments • Examine the system configuration settings and audit logs.	☐	☐	☒	☐	☐
	Applicability Notes						

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	This assessment is not the same as the vulnerability scans performed for Requirement 11.3.1 and 11.3.2. This requirement will be superseded by Requirement 6.4.2 after 31 March 2025 when Requirement 6.4.2 becomes effective.						
6.4.2	For public-facing web applications, an automated technical solution is deployed that continually detects and prevents web-based attacks, with at least the following: • Is installed in front of public-facing web applications and is configured to detect and prevent web-based attacks. • Actively running and up to date as applicable. • Generating audit logs. • Configured to either block web-based attacks or generate an alert that is immediately investigated.	• Examine the system configuration settings. • Examine audit logs. • Interview responsible personnel.	□	□	☒	□	□
	Applicability Notes						
	This new requirement will replace Requirement 6.4.1 once its effective date is reached. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
6.4.3	All payment page scripts that are loaded and executed in the consumer's browser are managed as follows:						
	• A method is implemented to confirm that each script is authorized.	• Examine policies and procedures. • Interview responsible personnel. • Examine inventory records. • Examine system configurations.	□	□	☒	□	□
	• A method is implemented to assure the integrity of each script.		□	□	☒	□	□
	• An inventory of all scripts is maintained with written justification as to why each is necessary.		□	□	☒	□	□
	Applicability Notes						
	This requirement applies to all scripts loaded from the entity's environment and scripts loaded from third and fourth parties. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.5 Changes to all system components are managed securely.							
6.5.1	Changes to all system components in the production environment are made according to established procedures that include: • Reason for, and description of, the change. • Documentation of security impact. • Documented change approval by authorized parties. • Testing to verify that the change does not adversely impact system security. • For bespoke and custom software changes, all updates are tested for compliance with Requirement 6.2.4 before being deployed into production. • Procedures to address failures and return to a secure state.	• Examine documented change control procedures. • Examine recent changes to system components and trace changes to change control documentation. • Examine change control documentation.	☐	☐	☒	☐	☐
6.5.2	Upon completion of a significant change, all applicable PCI DSS requirements are confirmed to be in place on all new or changed systems and networks, and documentation is updated as applicable.	• Examine documentation for significant changes. • Interview personnel. • Observe the affected systems/networks.	☐	☐	☒	☐	☐
	Applicability Notes						
	These significant changes should also be captured and reflected in the entity's annual PCI DSS scope confirmation activity per Requirement 12.5.2.						
6.5.3	Pre-production environments are separated from production environments and the separation is enforced with access controls.	• Examine policies and procedures. • Examine network documentation and configurations of network security controls. • Examine access control settings.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
6.5.4	Roles and functions are separated between production and pre-production environments to provide accountability such that only reviewed and approved changes are deployed.	• Examine policies and procedures. • Observe processes. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	In environments with limited personnel where individuals perform multiple roles or functions, this same goal can be achieved with additional procedural controls that provide accountability. For example, a developer may also be an administrator that uses an administrator-level account with elevated privileges in the development environment and, for their developer role, they use a separate account with user-level access to the production environment.						
6.5.5	Live PANs are not used in pre-production environments, except where those environments are included in the CDE and protected in accordance with all applicable PCI DSS requirements.	• Examine policies and procedures. • Observe testing processes. • Interview personnel. • Examine pre-production test data.	☐	☐	☒	☐	☐
6.5.6	Test data and test accounts are removed from system components before the system goes into production.	• Examine policies and procedures. • Observe testing processes for both off-the-shelf software and in-house applications. • Interview personnel. • Examine data and accounts for recently installed or updated off-the-shelf software and in-house applications.	☐	☐	☒	☐	☐

Implement Strong Access Control Measures

Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
7.1 Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood.							
7.1.1	All security policies and operational procedures that are identified in Requirement 7 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
7.1.2	Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	□	□	□	□
7.2 Access to system components and data is appropriately defined and assigned.							
7.2.1	An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	• Examine documented policies and procedures. • Interview personnel. • Examine access control model settings.	☒	□	□	□	□

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
7.2.2	Access is assigned to users, including privileged users, based on: • Job classification and function. • Least privileges necessary to perform job responsibilities.	• Examine policies and procedures. • Examine user access settings, including for privileged users. • Interview responsible management personnel. • Interview personnel responsible for assigning access.	☒	☐	☐	☐	☐
7.2.3	Required privileges are approved by authorized personnel.	• Examine policies and procedures. • Examine user IDs and assigned privileges. • Examine documented approvals.	☒	☐	☐	☐	☐
7.2.4	All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows: • At least once every six months. • To ensure user accounts and access remain appropriate based on job function. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	• Examine policies and procedures. • Interview responsible personnel. • Examine documented results of periodic reviews of user accounts.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement applies to all user accounts and related access privileges, including those used by personnel and third parties/vendors, and accounts used to access third-party cloud services. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
7.2.5	All application and system accounts and related access privileges are assigned and managed as follows: • Based on the least privileges necessary for the operability of the system or application. • Access is limited to the systems, applications, or processes that specifically require their use.	• Examine policies and procedures. • Examine privileges associated with system and application accounts. • Interview responsible personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
7.2.5.1	All access by application and system accounts and related access privileges are reviewed as follows: • Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1). • The application/system access remains appropriate for the function being performed. • Any inappropriate access is addressed. • Management acknowledges that access remains appropriate.	• Examine policies and procedures. • Examine the targeted risk analysis. • Interview responsible personnel. • Examine documented results of periodic reviews of system and application accounts and related privileges.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment						
7.2.6	All user access to query repositories of stored cardholder data is restricted as follows: • Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges. • Only the responsible administrator(s) can directly access or query repositories of stored CHD.	• Examine policies and procedures. • Interview personnel. • Examine configuration settings for querying repositories of stored cardholder data.	☐	☐	☒	☐	☐
	Applicability Notes *(cont.)*						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	This requirement applies to controls for user access to query repositories of stored cardholder data. See Requirements 7.2.5 and 7.2.5.1 and 8.6.1 through 8.6.3 for controls for application and system accounts.						
7.3 Access to system components and data is managed via an access control system(s).							
7.3.1	An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	• Examine vendor documentation. • Examine configuration settings.	☒	□	□	□	□
7.3.2	The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function.	• Examine vendor documentation. • Examine configuration settings.	☒	□	□	□	□
7.3.3	The access control system(s) is set to "deny all" by default.	• Examine vendor documentation. • Examine configuration settings.	☒	□	□	□	□

Requirement 8: Identify Users and Authenticate Access to System Components

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.1 Processes and mechanisms for identifying users and authenticating access to system components are defined and understood.							
8.1.1	All security policies and operational procedures that are identified in Requirement 8 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
8.1.2	Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account's lifecycle.							
8.2.1	All users are assigned a unique ID before access to system components or cardholder data is allowed.	• Interview responsible personnel. • Examine audit logs and other evidence.	☒	☐	☐	☐	☐
	Applicability Notes						
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.2.2	Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted. • Every action taken is attributable to an individual user.	• Examine user account lists on system components and applicable documentation. • Examine authentication policies and procedures. • Interview system administrators.	☒	□	□	□	□
	Applicability Notes						
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						
8.2.3	***Additional requirement for service providers only***						
8.2.4	Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	• Examine documented authorizations across various phases of the account lifecycle (additions, modifications, and deletions). • Examine system settings.	☒	□	□	□	□
	Applicability Notes						
	This requirement applies to all user accounts, including employees, contractors, consultants, temporary workers, and third-party vendors.						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.2.5	Access for terminated users is immediately revoked.	• Examine information sources for terminated users. • Review current user access lists. • Interview responsible personnel.	☒	☐	☐	☐	☐
8.2.6	Inactive user accounts are removed or disabled within 90 days of inactivity.	• Examine user accounts and last logon information. • Interview responsible personnel.	☒	☐	☐	☐	☐
8.2.7	Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows: • Enabled only during the time period needed and disabled when not in use. • Use is monitored for unexpected activity.	• Interview responsible personnel. • Examine documentation for managing accounts. • Examine evidence.	☒	☐	☐	☐	☐
8.2.8	If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	• Examine system configuration settings.	☒	☐	☐	☐	☐
	Applicability Notes						
	This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.						
8.3 Strong authentication for users and administrators is established and managed.							
8.3.1	All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	• Examine documentation describing the authentication factor(s) used. • For each type of authentication factor used with each type of system component, observe the authentication process.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Applicability Notes This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not supersede multi-factor authentication (MFA) requirements but applies to those in-scope systems not otherwise subject to MFA requirements. A digital certificate is a valid option for “something you have” if it is unique for a particular user						
8.3.2	Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	• Examine vendor documentation • Examine system configuration settings. • Examine repositories of authentication factors. • Examine data transmissions.	☒	□	□	□	□
8.3.3	User identity is verified before modifying any authentication factor.	• Examine procedures for modifying authentication factors. • Observe security personnel.	☒	□	□	□	□
8.3.4	Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user’s identity is confirmed. **Applicability Notes** This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	• Examine system configuration settings.	☒	□	□	□	□

PCI DSS Requirement		Expected Testing	Response ♦ (*Check one response for each requirement*)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.3.5	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	• Examine procedures for setting and resetting passwords/passphrases. • Observe security personnel.	☒	☐	☐	☐	☐
8.3.6	If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic characters.	• Examine system configuration settings.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is not intended to apply to: • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). • Application or system accounts, which are governed by requirements in section 8.6. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.						
8.3.7	Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.	• Examine system configuration settings.	☒	☐	☐	☐	☐
	Applicability Notes						
	This requirement is not intended to apply to user accounts within point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.3.8	Authentication policies and procedures are documented and communicated to all users including: • Guidance on selecting strong authentication factors. • Guidance for how users should protect their authentication factors. • Instructions not to reuse previously used passwords/passphrases. • Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.	• Examine procedures. • Interview personnel. • Review authentication policies and procedures that are distributed to users. • Interview users.	☒	☐	☐	☐	☐
8.3.9	If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	• Inspect system configuration settings.	☒	☐	☐	☐	☐
	Applicability Notes						
	This requirement applies to in-scope system components that are not in the CDE because these components are not subject to MFA requirements. This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement does not apply to service providers’ customer accounts but does apply to accounts for service provider personnel.						
8.3.10	***Additional requirement for service providers only***						
8.3.10.1	***Additional requirement for service providers only***						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.3.11	Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	• Examine authentication policies and procedures. • Interview security personnel. • Examine system configuration settings and/or observe physical controls, as applicable.	☒	□	□	□	□
8.4 Multi-factor authentication (MFA) is implemented to secure access into the CDE.							
8.4.1	MFA is implemented for all non-console access into the CDE for personnel with administrative access.	• Examine network and/or system configurations. • Observe administrator personnel logging into the CDE.	☒	□	□	□	□
	Applicability Notes						
	The requirement for MFA for non-console administrative access applies to all personnel with elevated or increased privileges accessing the CDE via a non-console connection—that is, via logical access occurring over a network interface rather than via a direct, physical connection. MFA is considered a best practice for non-console administrative access to in-scope system components that are not part of the CDE.						

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.4.2	MFA is implemented for all access into the CDE.	• Examine network and/or system configurations. • Observe personnel logging in to the CDE. • Examine evidence.	□	□	☒	□	□
	Applicability Notes This requirement does not apply to: • Application or system accounts performing automated functions. • User accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). MFA is required for both types of access specified in Requirements 8.4.2 and 8.4.3. Therefore, applying MFA to one type of access does not replace the need to apply another instance of MFA to the other type of access. If an individual first connects to the entity’s network via remote access, and then later initiates a connection into the CDE from within the network, per this requirement the individual would authenticate using MFA twice, once when connecting via remote access to the entity’s network and once when connecting via non-console administrative access from the entity’s network into the CDE. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity’s networks or systems as well as web-based access to an application or function. MFA for remote access into the CDE can be implemented at the network or system/application level; it does not have to be applied at both levels. For example, if MFA is used when a user connects to the CDE network, it does not have to be used when the user logs into each system or application within the CDE. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment*						

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.4.3	MFA is implemented for all remote network access originating from outside the entity's network that could access or impact the CDE as follows: • All remote access by all personnel, both users and administrators, originating from outside the entity's network. • All remote access by third parties and vendors.	• Examine network and/or system configurations for remote access servers and systems. • Observe personnel (for example, users and administrators) connecting remotely to the network.	☒	☐	☐	☐	☐
	Applicability Notes						
	The requirement for MFA for remote access originating from outside the entity's network applies to all user accounts that can access the network remotely, where that remote access leads to or could lead to access into the CDE. If remote access is to a part of the entity's network that is properly segmented from the CDE, such that remote users cannot access or impact the CDE, MFA for remote access to that part of the network is not required. However, MFA is required for any remote access to networks with access to the CDE and is recommended for all remote access to the entity's networks. The MFA requirements apply for all types of system components, including cloud, hosted systems, and on-premises applications, network security devices, workstations, servers, and endpoints, and includes access directly to an entity's networks or systems as well as web-based access to an application or function.						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.5 Multi-factor authentication (MFA) systems are configured to prevent misuse.							
8.5.1	MFA systems are implemented as follows: • The MFA system is not susceptible to replay attacks. • MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period. • At least two different types of authentication factors are used. • Success of all authentication factors is required before access is granted.	• Examine vendor system documentation. • Examine system configurations for the MFA implementation. • Interview responsible personnel and observe processes. • Observe personnel logging into system components in the CDE. • Observe personnel connecting remotely from outside the entity's network.	□	□	☒	□	□
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.6 Use of application and system accounts and associated authentication factors is strictly managed.							
8.6.1	If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user.	• Examine application and system accounts that can be used interactively. • Interview administrative personnel.	□	□	☒	□	□
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
8.6.2	Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code.	• Interview personnel. • Examine system development procedures. • Examine scripts, configuration/property files, and bespoke and custom source code for application and system accounts that can be used for interactive login.	□	□	☒	□	□
	Applicability Notes						
	Stored passwords/passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
8.6.3	Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases.	• Examine policies and procedures. • Examine the targeted risk analysis. • Interview responsible personnel. • Examine system configuration settings.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

Requirement 9: Restrict Physical Access to Cardholder Data

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.1 Processes and mechanisms for restricting physical access to cardholder data are defined and understood.							
9.1.1	All security policies and operational procedures that are identified in Requirement 9 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
9.1.2	Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	☐	☐	☐	☐
9.2 Physical access controls manage entry into facilities and systems containing cardholder data.							
9.2.1	Appropriate facility entry controls are in place to restrict physical access to systems in the CDE.	• Observe physical entry controls. • Interview responsible personnel.	☒	☐	☐	☐	☐
9.2.1.1	Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows: • Entry and exit points to/from sensitive areas within the CDE are monitored. • Monitoring devices or mechanisms are protected from tampering or disabling. • Collected data is reviewed and correlated with other entries. • Collected data is stored for at least three months, unless otherwise restricted by law.	• Observe locations where individual physical access to sensitive areas within the CDE occurs. • Observe the physical access control mechanisms and/or examine video cameras. • Interview responsible personnel.	☒	☐	☐	☐	☐

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.2.2	Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility.	• Interview responsible personnel. • Observe locations of publicly accessible network jacks.	☒	☐	☐	☐	☐
9.2.3	Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted.	• Interview responsible personnel. • Observe locations of hardware and lines.	☒	☐	☐	☐	☐
9.2.4	Access to consoles in sensitive areas is restricted via locking when not in use.	• Observe a system administrator's attempt to log into consoles in sensitive areas.	☒	☐	☐	☐	☐
9.3 Physical access for personnel and visitors is authorized and managed.							
9.3.1	Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including: • Identifying personnel. • Managing changes to an individual's physical access requirements. • Revoking or terminating personnel identification. • Limiting access to the identification process or system to authorized personnel.	• Examine documented procedures. • Observe identification methods, such as ID badges. • Observe processes.	☒	☐	☐	☐	☐
9.3.1.1	Physical access to sensitive areas within the CDE for personnel is controlled as follows: • Access is authorized and based on individual job function. • Access is revoked immediately upon termination. • All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination.	• Observe personnel in sensitive areas within the CDE. • Interview responsible personnel. • Examine physical access control lists. • Observe processes.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.3.2	Procedures are implemented for authorizing and managing visitor access to the CDE, including: • Visitors are authorized before entering. • Visitors are escorted at all times. • Visitors are clearly identified and given a badge or other identification that expires. • Visitor badges or other identification visibly distinguishes visitors from personnel.	• Examine documented procedures. • Observe processes when visitors are present in the CDE. • Interview personnel. • Observe the use of visitor badges or other identification.	☒	□	□	□	□
9.3.3	Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration.	• Observe visitors leaving the facility • Interview personnel.	☒	□	□	□	□
9.3.4	A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including: • The visitor's name and the organization represented. • The date and time of the visit. • The name of the personnel authorizing physical access. • Retaining the log for at least three months, unless otherwise restricted by law.	• Examine the visitor log. • Interview responsible personnel. • Examine visitor log storage locations.	☒	□	□	□	□
9.4 Media with cardholder data is securely stored, accessed, distributed, and destroyed.							
9.4.1	All media with cardholder data is physically secured.	• Examine documentation.	□	□	☒	□	□
9.4.1.1	Offline media backups with cardholder data are stored in a secure location.	• Examine documented procedures. • Examine logs or other documentation. • Interview responsible personnel at the storge location(s).	□	□	☒	□	□

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.4.1.2	The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months.	• Examine documented procedures, logs, or other documentation. • Interview responsible personnel at the storage location(s).	☐	☐	☒	☐	☐
9.4.2	All media with cardholder data is classified in accordance with the sensitivity of the data.	• Examine documented procedures. • Examine media logs or other documentation.	☐	☐	☒	☐	☐
9.4.3	Media with cardholder data sent outside the facility is secured as follows: • Media sent outside the facility is logged. • Media is sent by secured courier or other delivery method that can be accurately tracked. • Offsite tracking logs include details about media location.	• Examine documented procedures. • Interview personnel. • Examine records. • Examine offsite tracking logs for all media.	☐	☐	☒	☐	☐
9.4.4	Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals).	• Examine documented procedures. • Examine offsite media tracking logs. • Interview responsible personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	Individuals approving media movements should have the appropriate level of management authority to grant this approval. However, it is not specifically required that such individuals have “manager” as part of their title.						
9.4.5	Inventory logs of all electronic media with cardholder data are maintained.	• Examine documented procedures. • Examine electronic media inventory logs. • Interview responsible personnel.	☐	☐	☒	☐	☐

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.4.5.1	Inventories of electronic media with cardholder data are conducted at least once every 12 months.	• Examine documented procedures. • Examine electronic media inventory logs. • Interview responsible personnel.	☐	☐	☒	☐	☐
9.4.6	Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows: • Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. • Materials are stored in secure storage containers prior to destruction.	• Examine the periodic media destruction policy. • Observe processes. • Interview personnel. • Observe storage containers.	☐	☐	☒	☐	☐
	Applicability Notes						
	These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.						
9.4.7	Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following: • The electronic media is destroyed. • The cardholder data is rendered unrecoverable so that it cannot be reconstructed.	• Examine the periodic media destruction policy. • Observe the media destruction process. • Interview responsible personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	These requirements for media destruction when that media is no longer needed for business or legal reasons are separate and distinct from PCI DSS Requirement 3.2.1, which is for securely deleting cardholder data when no longer needed per the entity's cardholder data retention policies.						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.5 Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.							
9.5.1	POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following: • Maintaining a list of POI devices. • Periodically inspecting POI devices to look for tampering or unauthorized substitution. • Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.	• Examine documented policies and procedures.	☒	□	□	□	□
	Applicability Notes						
	These requirements apply to deployed POI devices used in card-present transactions (that is, a payment card form factor such as a card that is swiped, tapped, or dipped). This requirement is not intended to apply to manual PAN key-entry components such as computer keyboards. This requirement is recommended, but not required, for manual PAN key-entry components such as computer keyboards. This requirement does not apply to commercial off-the-shelf (COTS) devices (for example, smartphones or tablets), which are mobile merchant-owned devices designed for mass-market distribution.						
9.5.1.1	An up-to-date list of POI devices is maintained, including: • Make and model of the device. • Location of device. • Device serial number or other methods of unique identification.	• Examine the list of POI devices. • Observe POI devices and device locations. • Interview personnel.	☒	□	□	□	□
9.5.1.2	POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.	• Examine documented procedures. • Interview responsible personnel. • Observe inspection processes.	☒	□	□	□	□

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
9.5.1.2.1	The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	• Examine the targeted risk analysis. • Examine documented results of periodic device inspections. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
9.5.1.3	Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes: • Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices. • Procedures to ensure devices are not installed, replaced, or returned without verification. • Being aware of suspicious behavior around devices. • Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.	• Review training materials for personnel in POI environments. • Interview responsible personnel.	☒	☐	☐	☐	☐

Regularly Monitor and Test Networks

Requirement 10: Log and Monitor All Access to System Components and Cardholder Data

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.1 Processes and mechanisms for logging and monitoring all access to system components and cardholder data are defined and documented.							
10.1.1	All security policies and operational procedures that are identified in Requirement 10 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
10.1.2	Roles and responsibilities for performing activities in Requirement 10 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	□	□	□	□
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.							
10.2.1	Audit logs are enabled and active for all system components and cardholder data.	• Interview the system administrator. • Examine system configurations.	☒	□	□	□	□
10.2.1.1	Audit logs capture all individual user access to cardholder data.	• Examine audit log configurations. • Examine audit log data.	□	□	☒	□	□
10.2.1.2	Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	• Examine audit log configurations. • Examine audit log data.	☒	□	□	□	□
10.2.1.3	Audit logs capture all access to audit logs.	• Examine audit log configurations. • Examine audit log data.	☒	□	□	□	□
10.2.1.4	Audit logs capture all invalid logical access attempts.	• Examine audit log configurations. • Examine audit log data.	☒	□	□	□	□

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.2.1.5	Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	• Examine audit log configurations. • Examine audit log data.	☒	☐	☐	☐	☐
10.2.1.6	Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	• Examine audit log configurations. • Examine audit log data.	☒	☐	☐	☐	☐
10.2.1.7	Audit logs capture all creation and deletion of system-level objects.	• Examine audit log configurations. • Examine audit log data.	☒	☐	☐	☐	☐
10.2.2	Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	• Interview responsible personnel. • Examine audit log configurations. • Examine audit log data.	☒	☐	☐	☐	☐
10.3 Audit logs are protected from destruction and unauthorized modifications.							
10.3.1	Read access to audit logs files is limited to those with a job-related need.	• Interview system administrators • Examine system configurations and privileges.	☒	☐	☐	☐	☐
10.3.2	Audit log files are protected to prevent modifications by individuals.	• Examine system configurations and privileges. • Interview system administrators.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.3.3	Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	• Examine backup configurations or log files.	☒	☐	☐	☐	☐
10.3.4	File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	• Examine system settings. • Examine monitored files. • Examine results from monitoring activities.	☒	☐	☐	☐	☐
10.4 Audit logs are reviewed to identify anomalies or suspicious activity.							
10.4.1	The following audit logs are reviewed at least once daily: • All security events. • Logs of all system components that store, process, or transmit CHD and/or SAD. • Logs of all critical system components. • Logs of all servers and system components that perform security functions (for example, network security controls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers).	• Examine security policies and procedures. • Observe processes. • Interview personnel.	☒	☐	☐	☐	☐
10.4.1.1	Automated mechanisms are used to perform audit log reviews.	• Examine log review mechanisms. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
10.4.2	Logs of all other system components (those not specified in Requirement 10.4.1) are reviewed periodically.	• Examine security policies and procedures. • Examine documented results of log reviews. • Interview personnel.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Applicability Notes This requirement is applicable to all other in-scope system components not included in Requirement 10.4.1.						
10.4.2.1	The frequency of periodic log reviews for all other system components (not defined in Requirement 10.4.1) is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	• Examine the targeted risk analysis. • Examine documented results of periodic log reviews. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
10.4.3	Exceptions and anomalies identified during the review process are addressed.	• Examine security policies and procedures. • Observe processes. • Interview personnel.	☒	☐	☐	☐	☐
10.5 Audit log history is retained and available for analysis.							
10.5.1	Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	• Examine documented audit log retention policies and procedures. • Examine configurations of audit log history. • Examine audit logs. • Interview personnel. • Observe processes.	☒	☐	☐	☐	☐
10.6 Time-synchronization mechanisms support consistent time settings across all systems.							
10.6.1	System clocks and time are synchronized using time-synchronization technology.	• Examine system configuration settings.	☒	☐	☐	☐	☐
	Applicability Notes Keeping time-synchronization technology current includes managing vulnerabilities and patching the technology according to PCI DSS Requirements 6.3.1 and 6.3.3.						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.6.2	Systems are configured to the correct and consistent time as follows: • One or more designated time servers are in use. • Only the designated central time server(s) receives time from external sources. • Time received from external sources is based on International Atomic Time or Coordinated Universal Time (UTC). • The designated time server(s) accept time updates only from specific industry-accepted external sources. • Where there is more than one designated time server, the time servers peer with one another to keep accurate time. • Internal systems receive time information only from designated central time server(s).	• Examine system configuration settings for acquiring, distributing, and storing the correct time.	☒	☐	☐	☐	☐
10.6.3	Time synchronization settings and data are protected as follows: • Access to time data is restricted to only personnel with a business need. • Any changes to time settings on critical systems are logged, monitored, and reviewed.	• Examine system configurations and time-synchronization settings and logs. • Observe processes.	☒	☐	☐	☐	☐
10.7 Failures of critical security control systems are detected, reported, and responded to promptly.							
10.7.1	***Additional requirement for service providers only***						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.7.2	Failures of critical security control systems are detected, alerted, and addressed promptly, including but not limited to failure of the following critical security control systems: • Network security controls. • IDS/IPS. • Change-detection mechanisms. • Anti-malware solutions. • Physical access controls. • Logical access controls. • Audit logging mechanisms. • Segmentation controls (if used). • Audit log review mechanisms. • Automated security testing tools (if used).	• Examine documented processes. • Observe detection and alerting processes. • Interview personnel.	□	□	☒	□	□
	Applicability Notes						
	This requirement applies to all entities, including service providers, and will supersede Requirement 10.7.1 as of 31 March 2025. It includes two additional critical security control systems not in Requirement 10.7.1. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
10.7.3	Failures of any critical security controls systems are responded to promptly, including but not limited to: • Restoring security functions. • Identifying and documenting the duration (date and time from start to end) of the security failure. • Identifying and documenting the cause(s) of failure and documenting required remediation. • Identifying and addressing any security issues that arose during the failure. • Determining whether further actions are required as a result of the security failure. • Implementing controls to prevent the cause of failure from reoccurring. • Resuming monitoring of security controls.	• Examine documented processes . • Interview personnel. • Examine records related to critical security control systems failures.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement applies only when the entity being assessed is a service provider until 31 March 2025, after which this requirement will apply to all entities. *This is a current v3.2.1 requirement that applies to service providers only. However, this requirement is a best practice for all other entities until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

Requirement 11: Test Security of Systems and Networks Regularly

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.1 Processes and mechanisms for regularly testing security of systems and networks are defined and understood.							
11.1.1	All security policies and operational procedures that are identified in Requirement 11 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	• Examine documentation. • Interview personnel.	☒	□	□	□	□
11.1.2	Roles and responsibilities for performing activities in Requirement 11 are documented, assigned, and understood.	• Examine documentation. • Interview responsible personnel.	☒	□	□	□	□

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.2 Wireless access points are identified and monitored, and unauthorized wireless access points are addressed.							
11.2.1	Authorized and unauthorized wireless access points are managed as follows: • The presence of wireless (Wi-Fi) access points is tested for. • All authorized and unauthorized wireless access points are detected and identified. • Testing, detection, and identification occurs at least once every three months. • If automated monitoring is used, personnel are notified via generated alerts.	• Examine policies and procedures. • Examine the methodology(ies) in use and the resulting documentation. • Interview personnel. • Examine wireless assessment results. • Examine configuration settings.	☒	□	□	□	□
	Applicability Notes						
	The requirement applies even when a policy exists that prohibits the use of wireless technology since attackers do not read and follow company policy. Methods used to meet this requirement must be sufficient to detect and identify both authorized and unauthorized devices, including unauthorized devices attached to devices that themselves are authorized.						
11.2.2	An inventory of authorized wireless access points is maintained, including a documented business justification.	• Examine documentation.	☒	□	□	□	□

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.3 External and internal vulnerabilities are regularly identified, prioritized, and addressed.							
11.3.1	Internal vulnerability scans are performed as follows: • At least once every three months. • High-risk and critical vulnerabilities (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are performed that confirm all high-risk and critical vulnerabilities (as noted above) have been resolved. • Scan tool is kept up to date with latest vulnerability information. • Scans are performed by qualified personnel and organizational independence of the tester exists.	• Examine internal scan report results. • Examine scan tool configurations. • Interview responsible personnel.	☒	☐	☐	☐	☐
	Applicability Notes						
	It is not required to use a QSA or ASV to conduct internal vulnerability scans. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a network administrator should not be responsible for scanning the network), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.3.1.1	All other applicable vulnerabilities (those not ranked as high-risk or critical (per the entity's vulnerability risk rankings defined at Requirement 6.3.1) are managed as follows: • Addressed based on the risk defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. • Rescans are conducted as needed.	• Examine the targeted risk analysis. • Interview responsible personnel. • Examine internal scan report results or other documentation.	□	□	☒	□	□
	Applicability Notes						
	The timeframe for addressing lower-risk vulnerabilities is subject to the results of a risk analysis per Requirement 12.3.1 that includes (minimally) identification of assets being protected, threats, and likelihood and/or impact of a threat being realized. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.3.1.2	Internal vulnerability scans are performed via authenticated scanning as follows:						
	• Systems that are unable to accept credentials for authenticated scanning are documented.	• Examine documentation. • Examine scan tool configurations. • Examine scan report results. • Interview personnel. • Examine accounts used for authenticated scanning.	□	□	☒	□	□
	• Sufficient privileges are used for those systems that accept credentials for scanning.		□	□	☒	□	□
	• If accounts used for authenticated scanning can be used for interactive login, they are managed in accordance with Requirement 8.2.2.		□	□	☒	□	□
	Applicability Notes						
	The authenticated scanning tools can be either host-based or network-based. “Sufficient” privileges are those needed to access system resources such that a thorough scan can be conducted that detects known vulnerabilities. This requirement does not apply to system components that cannot accept credentials for scanning. Examples of systems that may not accept credentials for scanning include some network and security appliances, mainframes, and containers. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
11.3.1.3	Internal vulnerability scans are performed after any significant change as follows: • High-risk and critical vulnerabilities (per the entity’s vulnerability risk rankings defined at Requirement 6.3.1) are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine change control documentation. • Interview personnel. • Examine internal scan and rescan report as applicable. • Interview personnel.	☒	□	□	□	□
	Applicability Notes						
	Authenticated internal vulnerability scanning per Requirement 11.3.1.2 is not required for scans performed after significant changes.						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.3.2	External vulnerability scans are performed as follows: • At least once every three months. • By a PCI SSC Approved Scanning Vendor (ASV) • Vulnerabilities are resolved and *ASV Program Guide* requirements for a passing scan are met. • Rescans are performed as needed to confirm that vulnerabilities are resolved per the *ASV Program Guide* requirements for a passing scan.	• Examine ASV scan reports. •	☒	☐	☐	☐	☐
	Applicability Notes						
	For initial PCI DSS compliance, it is not required that four passing scans be completed within 12 months if the assessor verifies: 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring scanning at least once every three months, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). However, for subsequent years after the initial PCI DSS assessment, passing scans at least every three months must have occurred. ASV scanning tools can scan a vast array of network types and topologies. Any specifics about the target environment (for example, load balancers, third-party providers, ISPs, specific configurations, protocols in use, scan interference) should be worked out between the ASV and scan customer. Refer to the *ASV Program Guide* published on the PCI SSC website for scan customer responsibilities, scan preparation, etc.						
11.3.2.1	External vulnerability scans are performed after any significant change as follows: • Vulnerabilities that are scored 4.0 or higher by the CVSS are resolved. • Rescans are conducted as needed. • Scans are performed by qualified personnel and organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine change control documentation. • Interview personnel. • Examine external scan, and as applicable rescan reports.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.4 External and internal penetration testing is regularly performed, and exploitable vulnerabilities and security weaknesses are corrected.							
11.4.1	A penetration testing methodology is defined, documented, and implemented by the entity, and includes: • Industry-accepted penetration testing approaches. • Coverage for the entire CDE perimeter and critical systems. • Testing from both inside and outside the network. • Testing to validate any segmentation and scope-reduction controls. • Application-layer penetration testing to identify, at a minimum, the vulnerabilities listed in Requirement 6.2.4. • Network-layer penetration tests that encompass all components that support network functions as well as operating systems. • Review and consideration of threats and vulnerabilities experienced in the last 12 months. • Documented approach to assessing and addressing the risk posed by exploitable vulnerabilities and security weaknesses found during penetration testing. • Retention of penetration testing results and remediation activities results for at least 12 months.	• Examine documentation. • Interview personnel.	☒	☐	☐	☐	☐
	Applicability Notes *(cont.)*						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
	Testing from inside the network (or “internal penetration testing”) means testing from both inside the CDE and into the CDE from trusted and untrusted internal networks. Testing from outside the network (or “external penetration testing”) means testing the exposed external perimeter of trusted networks, and critical systems connected to or accessible to public network infrastructures.						
11.4.2	Internal penetration testing is performed: • Per the entity’s defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party • Organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine scope of work. • Examine results from the most recent external penetration test. • Interview responsible personnel.	☒	☐	☐	☐	☐
11.4.3	External penetration testing is performed: • Per the entity’s defined methodology. • At least once every 12 months. • After any significant infrastructure or application upgrade or change. • By a qualified internal resource or qualified external third-party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine scope of work. • Examine results from the most recent external penetration test. • Interview responsible personnel.	☒	☐	☐	☐	☐
11.4.4	Exploitable vulnerabilities and security weaknesses found during penetration testing are corrected as follows: • In accordance with the entity’s assessment of the risk posed by the security issue as defined in Requirement 6.3.1. • Penetration testing is repeated to verify the corrections.	• Examine penetration testing results.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.4.5	If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows: • At least once every 12 months and after any changes to segmentation controls/methods • Covering all segmentation controls/methods in use. • According to the entity's defined penetration testing methodology. • Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems. • Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3). • Performed by a qualified internal resource or qualified external third party. • Organizational independence of the tester exists (not required to be a QSA or ASV).	• Examine segmentation controls. • Review penetration-testing methodology. • Examine the results from the most recent penetration test. • Interview responsible personnel.	☒	□	□	□	□
11.4.6	***Additional requirement for service providers only.***						
11.4.7	***Additional requirement for multi-tenant service providers only.***						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.5 Network intrusions and unexpected file changes are detected and responded to.							
11.5.1	Intrusion-detection and/or intrusion-prevention techniques are used to detect and/or prevent intrusions into the network as follows: • All traffic is monitored at the perimeter of the CDE. • All traffic is monitored at critical points in the CDE. • Personnel are alerted to suspected compromises. • All intrusion-detection and prevention engines, baselines, and signatures are kept up to date.	• Examine system configurations and network diagrams. • Examine system configurations. • Interview responsible personnel. • Examine vendor documentation.	☒	☐	☐	☐	☐
11.5.1.1	***Additional requirement for service providers only.***						
11.5.2	A change-detection mechanism (for example, file integrity monitoring tools) is deployed as follows: • To alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files. • To perform critical file comparisons at least once weekly.	• Examine system settings for the change-detection mechanism. • Examine monitored files. • Examine results from monitoring activities.	☒	☐	☐	☐	☐
	Applicability Notes						
	For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).						

PCI DSS Requirement		Expected Testing	Response ♦ (*Check one response for each requirement*)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
11.6 Unauthorized changes on payment pages are detected and responded to.							
11.6.1	A change- and tamper-detection mechanism is deployed as follows:						
	• To alert personnel to unauthorized modification (including indicators of compromise, changes, additions, and deletions) to the HTTP headers and the contents of payment pages as received by the consumer browser.	• Examine system settings and mechanism configuration settings. • Examine monitored payment pages. • Examine results from monitoring activities. • Examine the mechanism configuration settings. • Examine configuration settings. • Interview responsible personnel. • If applicable, examine the targeted risk analysis.	□	□	☒	□	□
	• The mechanism is configured to evaluate the received HTTP header and payment page.		□	□	☒	□	□
	• The mechanism functions are performed as follows: – At least once every seven days **OR** – Periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).		□	□	☒	□	□
	Applicability Notes						
	The intention of this requirement is not that an entity install software in the systems or browsers of its consumers, but rather that the entity uses techniques such as those described under Examples in the PCI DSS Guidance column to prevent and detect unexpected script activities. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

Maintain an Information Security Policy

Requirement 12: Support Information Security with Organizational Policies and Programs

PCI DSS Requirement		Expected Testing	Response[♦] *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.1 A comprehensive information security policy that governs and provides direction for protection of the entity's information assets is known and current.							
12.1.1	An overall information security policy is: • Established. • Published. • Maintained. • Disseminated to all relevant personnel, as well as to relevant vendors and business partners.	• Examine the information security policy. • Interview personnel.	☒	□	□	□	□
12.1.2	The information security policy is: • Reviewed at least once every 12 months. • Updated as needed to reflect changes to business objectives or risks to the environment	• Examine the information security policy. • Interview responsible personnel.	☒	□	□	□	□
12.1.3	The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.	• Examine the information security policy. • Interview responsible personnel. • Examine documented evidence.	☒	□	□	□	□
12.1.4	Responsibility for information security is formally assigned to a Chief Information Security Officer or other information security knowledgeable member of executive management.	• Examine the information security policy.	☒	□	□	□	□

[♦] *Refer to the "Requirement Responses" section (page v) for information about these response options.*

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.2 Acceptable use policies for end-user technologies are defined and implemented.							
12.2.1	Acceptable use policies for end-user technologies are documented and implemented, including: • Explicit approval by authorized parties. • Acceptable uses of the technology. • List of products approved by the company for employee use, including hardware and software.	• Examine acceptable use policies. • Interview responsible personnel.	☒	□	□	□	□
	Applicability Notes Examples of end-user technologies for which acceptable use policies are expected include, but are not limited to, remote access and wireless technologies, laptops, tablets, mobile phones, and removable electronic media, e-mail usage, and Internet usage.						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.3 Risks to the cardholder data environment are formally identified, evaluated, and managed.							
12.3.1	Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed • Performance of updated risk analyses when needed, as determined by the annual review.	• Examine documented policies and procedures.	□	□	☒	□	□
	Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
12.3.2	***This requirement is specific to the customized approach and does not apply to entities completing a self-assessment questionnaire.***						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.3.3	Cryptographic cipher suites and protocols in use are documented and reviewed at least once every 12 months, including at least the following: • An up-to-date inventory of all cryptographic cipher suites and protocols in use, including purpose and where used. • Active monitoring of industry trends regarding continued viability of all cryptographic cipher suites and protocols in use. • A documented strategy to respond to anticipated changes in cryptographic vulnerabilities.	• Examine documentation. • Interview personnel.	□	□	☒	□	□
	Applicability Notes						
	The requirement applies to all cryptographic suites and protocols used to meet PCI DSS requirements. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.3.4	Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following: • Analysis that the technologies continue to receive security fixes from vendors promptly. • Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance. • Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology. • Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.	• Examine documentation. • Interview personnel.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment						
12.4 PCI DSS compliance is managed.							
12.4.1	***Additional requirement for service providers only.***						
12.4.2	***Additional requirement for service providers only.***						
12.4.2.1	***Additional requirement for service providers only.***						
12.5 PCI DSS scope is documented and validated.							
12.5.1	An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.	• Examine the inventory. • Interview personnel.	☒	☐	☐	☐	☐

<table>
<tr><th colspan="2" rowspan="2">PCI DSS Requirement</th><th rowspan="2">Expected Testing</th><th colspan="5">Response ♦
(Check one response for each requirement)</th></tr>
<tr><th>In Place</th><th>In Place with CCW</th><th>Not Applicable</th><th>Not Tested</th><th>Not in Place</th></tr>
<tr><td><b>12.5.2</b></td><td>PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.</td><td>• Examine documented results of scope reviews.
• Interview personnel.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td><b><i>At a minimum, the scoping validation includes:</i></b></td><td colspan="6"></td></tr>
<tr><td></td><td>• Identifying all data flows for the various payment stages (for example, authorization, capture settlement, chargebacks, and refunds) and acceptance channels (for example, card-present, card-not-present, and e-commerce).</td><td rowspan="7">• Examine documented results of scope reviews.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Updating all data-flow diagrams per requirement 1.2.4.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Identifying all locations where account data is stored, processed, and transmitted, including but not limited to: 1) any locations outside of the currently defined CDE, 2) applications that process CHD, 3) transmissions between systems and networks, and 4) file backups.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Identifying all system components in the CDE, connected to the CDE, or that could impact security of the CDE.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Identifying all segmentation controls in use and the environment(s) from which the CDE is segmented, including justification for environments being out of scope.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Identifying all connections from third-party entities with access to the CDE.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
<tr><td></td><td>• Confirming that all identified data flows, account data, system components, segmentation controls, and connections from third parties with access to the CDE are included in scope.</td><td>☒</td><td>☐</td><td>☐</td><td>☐</td><td>☐</td></tr>
</table>

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.5.2 *(cont.)*	**Applicability Notes** This annual confirmation of PCI DSS scope is an activity expected to be performed by the entity under assessment, and is not the same, nor is it intended to be replaced by, the scoping confirmation performed by the entity's assessor during the annual assessment.						
12.5.2.1	***Additional requirement for service providers only.***						
12.5.3	***Additional requirement for service providers only.***						
12.6 Security awareness education is an ongoing activity.							
12.6.1	A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.	• Examine the security awareness program.	☒	□	□	□	□
12.6.2	The security awareness program is: • Reviewed at least once every 12 months, and • Updated as needed to address any new threats and vulnerabilities that may impact the security of the entity's CDE, or the information provided to personnel about their role in protecting cardholder data. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	• Examine security awareness program content. • Examine evidence of reviews. • Interview personnel.	□	□	☒	□	□
12.6.3	Personnel receive security awareness training as follows: • Upon hire and at least once every 12 months. • Multiple methods of communication are used. • Personnel acknowledge at least once every 12 months that they have read and understood the information security policy and procedures.	• Examine security awareness program records. • Interview applicable personnel. • Examine the security awareness program materials. • Examine personnel acknowledgements.	☒	□	□	□	□

PCI DSS Requirement		**Expected Testing**	**Response ♦** *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.6.3.1	Security awareness training includes awareness of threats and vulnerabilities that could impact the security of the CDE, including but not limited to: • Phishing and related attacks. • Social engineering.	• Examine security awareness training content.	□	□	☒	□	□
	Applicability Notes						
	See Requirement 5.4.1 in PCI DSS for guidance on the difference between technical and automated controls to detect and protect users from phishing attacks, and this requirement for providing users security awareness training about phishing and social engineering. These are two separate and distinct requirements, and one is not met by implementing controls required by the other one. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*						
12.6.3.2	Security awareness training includes awareness about the acceptable use of end-user technologies in accordance with Requirement 12.2.1.	• Examine security awareness training content.	□	□	☒	□	□
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
12.7 Personnel are screened to reduce risks from insider threats.							
12.7.1	Potential personnel who will have access to the CDE are screened, within the constraints of local laws, prior to hire to minimize the risk of attacks from internal sources.	• Interview responsible Human Resource department management personnel.	☒	□	□	□	□
	Applicability Notes						
	For those potential personnel to be hired for positions such as store cashiers, who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.						

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.8 Risk to information assets associated with third-party service provider (TPSP) relationships is managed.							
12.8.1	A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.	• Examine policies and procedures. • Examine list of TPSPs.	☒	☐	☐	☐	☐
	Applicability Notes						
	The use of a PCI DSS compliant TPSP does not make an entity PCI DSS compliant, nor does it remove the entity's responsibility for its own PCI DSS compliance.						
12.8.2	Written agreements with TPSPs are maintained as follows: • Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE. • Written agreements include acknowledgments from TPSPs that they are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that they could impact the security of the entity's CDE.	• Examine policies and procedures. • Examine written agreements with TPSPs.	☒	☐	☐	☐	☐
	Applicability Notes						
	The exact wording of an acknowledgment will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement. Evidence that a TPSP is meeting PCI DSS requirements (for example, a PCI DSS Attestation of Compliance (AOC) or a declaration on a company's website) is not the same as a written agreement specified in this requirement.						
12.8.3	An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.	• Examine policies and procedures. • Examine evidence. • Interview responsible personnel.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.8.4	A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☒	□	□	□	□
	Applicability Notes						
	Where an entity has an agreement with a TPSP for meeting PCI DSS requirements on behalf of the entity (for example, via a firewall service), the entity must work with the TPSP to make sure the applicable PCI DSS requirements are met. If the TPSP does not meet those applicable PCI DSS requirements, then those requirements are also "not in place" for the entity.						
12.8.5	Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.	• Examine policies and procedures. • Examine documentation. • Interview responsible personnel.	☒	□	□	□	□
12.9 Third-party service providers (TPSPs) support their customers' PCI DSS compliance.							
12.9.1	***Additional requirement for service providers only.***						
12.9.2	***Additional requirement for service providers only.***						

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.							
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☒	☐	☐	☐	☐
12.10.2	At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	• Interview personnel. • Examine documentation.	☒	☐	☐	☐	☐
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	• Interview responsible personnel. • Examine documentation.	☒	☐	☐	☐	☐
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	• Interview incident response personnel. • Examine training documentation.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.10.4.1	The frequency of periodic training for incident response personnel is defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1.	- Examine the targeted risk analysis.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						
12.10.5	The security incident response plan includes monitoring and responding to alerts from security monitoring systems, including but not limited to: • Intrusion-detection and intrusion-prevention systems. • Network security controls. • Change-detection mechanisms for critical files. • The change-and tamper-detection mechanism for payment pages. *This bullet is a best practice until its effective date; refer to Applicability Notes below for details.* • Detection of *unauthorized* wireless access points.	• Examine documentation. • Observe incident response processes.	☐	☐	☒	☐	☐
	Applicability Notes						
	The bullet above (for monitoring and responding to alerts from a change- and tamper-detection mechanism for payment pages) is a best practice until 31 March 2025, after which it will be required as part of Requirement 12.10.5 and must be fully considered during a PCI DSS assessment.						
12.10.6	The security incident response plan is modified and evolved according to lessons learned and to incorporate industry developments.	• Examine policies and procedures. • Examine the security incident response plan. • Interview responsible personnel.	☒	☐	☐	☐	☐

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.10.7	Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable. • Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.	• Examine documented incident response procedures. • Interview personnel. • Examine records of response actions.	□	□	☒	□	□
	Applicability Notes						
	This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.						

Appendix A: Additional PCI DSS Requirements

Appendix A1: Additional PCI DSS Requirements for Multi-Tenant Service Providers

This Appendix is not used for merchant assessments.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections

PCI DSS Requirement		Expected Testing	**Response** ♦ *(Check one response for each requirement)*				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
A2.1 POI terminals using SSL and/or early TLS are not susceptible to known SSL/TLS exploits.							
A2.1.1	Where POS POI terminals at the merchant or payment acceptance location use SSL and/or early TLS, the entity confirms the devices are not susceptible to any known exploits for those protocols.	• Examine documentation (for example, vendor documentation, system/network configuration details) that verifies the devices are not susceptible to any known exploits for SSL/early TLS.	☐	☐	☒	☐	☐
	Applicability Notes						
	This requirement is intended to apply to the entity with the POS POI terminal, such as a merchant. This requirement is not intended for service providers who serve as the termination or connection point to those POS POI terminals. Requirements A2.1.2 and A2.1.3 apply to POS POI service providers. The allowance for POS POI terminals that are not currently susceptible to exploits is based on currently known risks. If new exploits are introduced to which POS POI terminals are susceptible, the POS POI terminals will need to be updated immediately.						
A2.1.2	***Additional requirement for service providers only.***						
A2.1.3	***Additional requirement for service providers only.***						

♦ *Refer to the "Requirement Responses" section (page v) for information about these response options.*

Appendix A3: Designated Entities Supplemental Validation (DESV)

This Appendix applies only to entities designated by a payment brand(s) or acquirer as requiring additional validation of existing PCI DSS requirements. Entities required to validate to this Appendix should use the DESV Supplemental Reporting Template and Supplemental Attestation of Compliance for reporting and consult with the applicable payment brand and/or acquirer for submission procedures.

Appendix B: Compensating Controls Worksheet

This Appendix must be completed to define compensating controls for any requirement where In Place with CCW was selected.

Note: *Only entities that have a legitimate and documented technological or business constraint can consider the use of compensating controls to achieve compliance.*

Refer to Appendices B and C in PCI DSS for information about compensating controls and guidance on how to complete this worksheet.

Requirement Number and Definition:

	Information Required	Explanation
1. Constraints	Document the legitimate technical or business constraints precluding compliance with the original requirement.	
2. Definition of Compensating Controls	Define the compensating controls: explain how they address the objectives of the original control and the increased risk, if any.	
3. Objective	Define the objective of the original control.	
	Identify the objective met by the compensating control. ***Note:*** *This can be, but is not required to be, the stated Customized Approach Objective listed for this requirement in PCI DSS.*	
4. Identified Risk	Identify any additional risk posed by the lack of the original control.	
5. Validation of Compensating Controls	Define how the compensating controls were validated and tested.	
6. Maintenance	Define process(es) and controls in place to maintain compensating controls.	

Appendix C: Explanation of Requirements Noted as Not Applicable

This Appendix must be completed for each requirement where Not Applicable was selected.

Requirement	Reason Requirement is Not Applicable
Example:	
Requirement 3.5.1	*Account data is never stored electronically*
1.2.6 1.3.3 1.4.4	There are no insecure services in use. There are no wireless networks within the cardholder data environment in scope. The City of Coral Gables does not store cardholder information.
2.3.1, 2.3.2 2.2.5	The City of Coral Gables does not allow access into the cardholder environment through the use of wireless access points. There are no insecure services in use.
3.2.1 - 3.7.8	The City of Coral Gables does not store cardholder information.
4.2.1.d 4.2.1.1 4.2.1.2 4.2.2	The City of Coral Gables does not transmit PAN over open, public networks. This requirement is a best practice until 31 March 2025. The City of Coral Gables does not send cardholder information through the use of wireless technologies. The City of Coral Gables does not send cardholder information through the use of end-user messaging technologies.
5.2.3 5.3.2.1 5.3.3, 5.4.1	All computers have antivirus/antimalware software installed. Real-time scans performed. This requirement is a best practice until 31 March 2025.
6.2.1-6.2.4, 6.4.1-6.5.6 6.3.2	The City of Coral Gables does not develop web applications that can affect the cardholder environment. This requirement is a best practice until 31 March 2025.
7.2.4-7.2.5.1 7.2.6	This requirement is a best practice until 31 March 2025. The City of Coral Gables does not store cardholder information.
8.3.6, 8.4.2, 8.5.1, 8.6.1, 8.6.2, 8.6.3	This requirement is a best practice until 31 March 2025.
9.4.1-9.4.7 9.5.1.2.1	The City of Coral Gables does not store cardholder information. This requirement is a best practice until 31 March 2025.
10.2.1.1 10.4.1.1, 10.4.2.1, 10.7.2, 10.7.3	The City of Coral Gables does not store cardholder information. This requirement is a best practice until 31 March 2025.
11.3.1.1, 11.3.1.2, 11.6.1	This requirement is a best practice until 31 March 2025.
12.3.1, 12.3.3, 12.3.4, 12.6.2, 12.6.3.1, 12.10.4.1, 12.10.7	This requirement is a best practice until 31 March 2025.

Requirement	Reason Requirement is Not Applicable

Appendix D: Explanation of Requirements Noted as Not Tested

This Appendix must be completed for each requirement where Not Tested was selected.

Requirement	Description of Requirement(s) Not Tested	Describe why Requirement(s) was Excluded from the Assessment
Examples:		
Requirement 10	*No requirements from Requirement 10 were tested.*	*This assessment only covers requirements in Milestone 1 of the Prioritized Approach.*
Requirements 1-8, 10-12	*Only Requirement 9 was reviewed for this assessment. All other requirements were excluded.*	*Company is a physical hosting provider (CO-LO), and only physical security controls were considered for this assessment.*

Section 3: Validation and Attestation Details

Part 3. PCI DSS Validation

This AOC is based on results noted in SAQ D (Section 2), dated (Self-assessment completion date *2024-10-15***).**

Indicate below whether a full or partial PCI DSS assessment was completed:

☒ **Full** – All requirements have been assessed therefore no requirements were marked as Not Tested in the SAQ.

□ **Partial** – One or more requirements have not been assessed and were therefore marked as Not Tested in the SAQ. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the SAQ D noted above, each signatory identified in any of Parts 3b–3d, as applicable, assert(s) the following compliance status for the merchant identified in Part 2 of this document.

Select one:

☒ **Compliant:** All sections of the PCI DSS SAQ are complete, and all assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *The City of Coral Gables* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above.

□ **Non-Compliant:** Not all sections of the PCI DSS SAQ are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating, thereby *(Merchant Company Name)* has not demonstrated compliance with the PCI DSS requirements included in this SAQ.

Target Date for Compliance: *YYYY-MM-DD*

A merchant submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted *before completing Part 4.*

□ **Compliant but with Legal exception:** One or more assessed requirements in the PCI DSS SAQ are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either 1) In Place, 2) In Place with CCW, or 3) Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Merchant Company Name)* has demonstrated compliance with all PCI DSS requirements included in this SAQ except those noted as Not Tested above or as Not in Place due to a legal restriction.

This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3a. Merchant Acknowledgement

Signatory(s) confirms:
(Select all that apply)

☒	PCI DSS Self-Assessment Questionnaire D, Version 4.0 was completed according to the instructions therein.
☒	All information within the above-referenced SAQ and in this attestation fairly represents the results of the merchant's assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the merchant's environment.

Part 3b. Merchant Attestation

DocuSigned by:
Raimundo Rodulfo
FCC8D8CB914E43F...

Signature of Merchant Executive Officer ↑	*Date:* ***2024-10-15***
Merchant Executive Officer Name: **Raimundo Rudolfo**	*Title:* **Director of Information Technology**

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this assessment, indicate the role performed:	☒ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA ↑	*Date:* ***2024-10-15***

Lead QSA Name: **Akash Desai**

Signature of Duly Authorized Officer of QSA Company ↑	*Date:* ***2024-10-15***
Duly Authorized Officer Name: **Silka M Gonzalez**	*QSA Company:* **ERMProtect**

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has a Non-Compliant status noted in Section 3.

If asked to complete this section, select the appropriate response for “Compliant to PCI DSS Requirements” for each requirement below. For any “No” responses, include the date the merchant expects to be compliant with the requirement and a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	**Description of Requirement**	**Compliant to PCI DSS Requirements** (Select One)		**Remediation Date and Actions** (If “NO” selected for any Requirement)
		YES	**NO**	
1	Install and maintain network security controls	☒	□	
2	Apply secure configurations to all system components	☒	□	
3	Protect stored account data	☒	□	
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☒	□	
5	Protect all systems and networks from malicious software	☒	□	
6	Develop and maintain secure systems and software	☒	□	
7	Restrict access to system components and cardholder data by business need to know	☒	□	
8	Identify users and authenticate access to system components	☒	□	
9	Restrict physical access to cardholder data	☒	□	
10	Log and monitor all access to system components and cardholder data	☒	□	
11	Test security systems and networks regularly	☒	□	
12	Support information security with organizational policies and programs	☒	□	
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/Early TLS for Card-Present POS POI Terminal Connections	☒	□	

City of Coral Gables

COMMUNITY RECREATION

Emergency Management Hurricane Plan 2025

Table of Contents

City of Coral Gables
COMMUNITY RECREATION
AFTER HOURS EMERGENCY CONTACTS
Procedure Flowchart

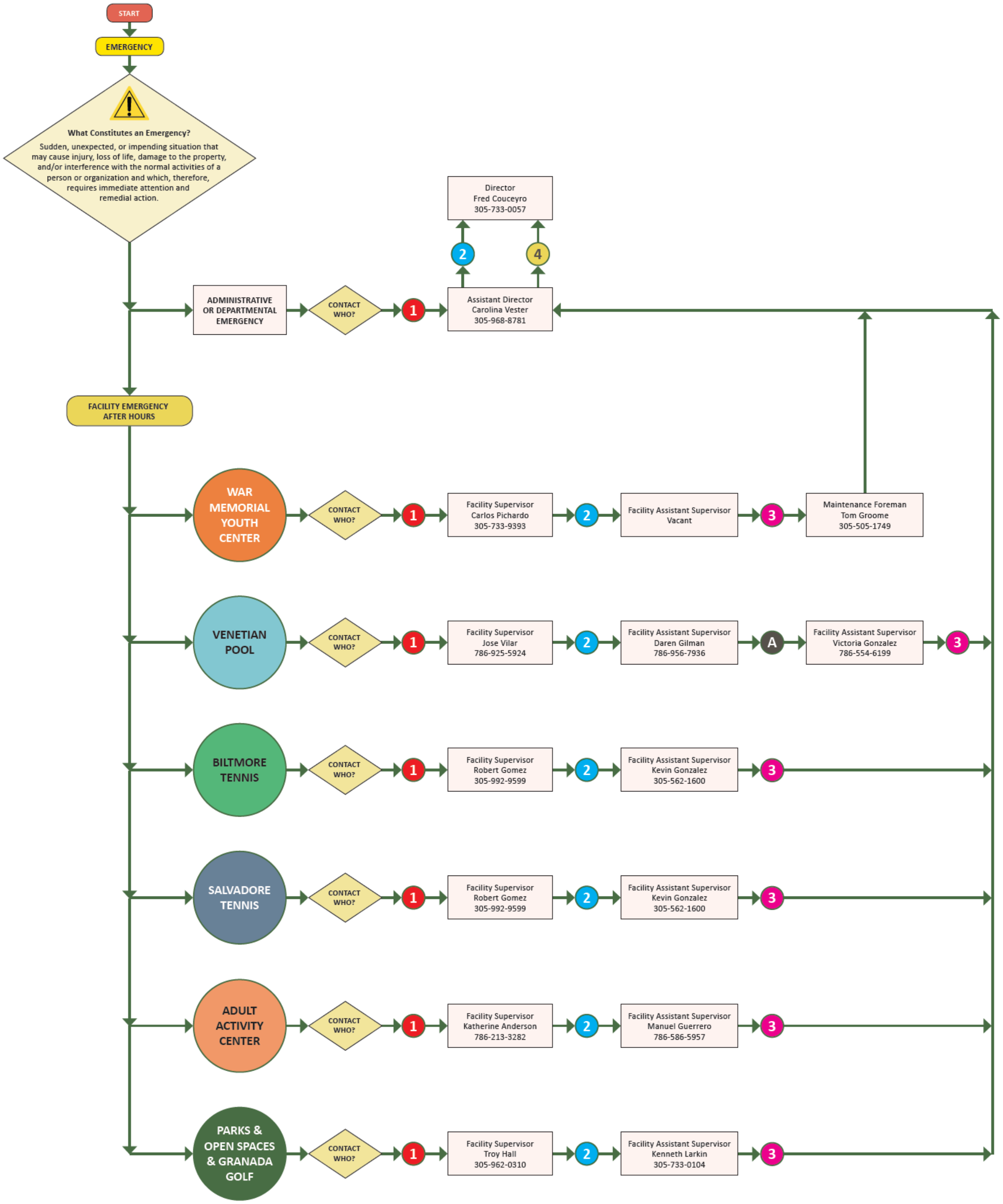

START
EMERGENCY
What Constitutes an Emergency?
Sudden, unexpected, or impending situation that may cause injury, loss of life, damage to the property, and/or interference with the normal activities of a person or organization and which, therefore, requires immediate attention and remedial action.
ADMINISTRATIVE OR DEPARTMENTAL EMERGENCY
CONTACT WHO?
1
Assistant Director Carolina Vester 305-968-8781
2
4
Director Fred Couceyro 305-733-0057
FACILITY EMERGENCY AFTER HOURS
WAR MEMORIAL YOUTH CENTER
CONTACT WHO?
1
Facility Supervisor Carlos Pichardo 305-733-9393
2
Facility Assistant Supervisor Vacant
3
Maintenance Foreman Tom Groome 305-505-1749
VENETIAN POOL
CONTACT WHO?
1
Facility Supervisor Jose Vilar 786-925-5924
2
Facility Assistant Supervisor Daren Gilman 786-956-7936
A
Facility Assistant Supervisor Victoria Gonzalez 786-554-6199
3
BILTMORE TENNIS
CONTACT WHO?
1
Facility Supervisor Robert Gomez 305-992-9599
2
Facility Assistant Supervisor Kevin Gonzalez 305-562-1600
3
SALVADORE TENNIS
CONTACT WHO?
1
Facility Supervisor Robert Gomez 305-992-9599
2
Facility Assistant Supervisor Kevin Gonzalez 305-562-1600
3
ADULT ACTIVITY CENTER
CONTACT WHO?
1
Facility Supervisor Katherine Anderson 786-213-3282
2
Facility Assistant Supervisor Manuel Guerrero 786-586-5957
3
PARKS & OPEN SPACES & GRANADA GOLF
CONTACT WHO?
1
Facility Supervisor Troy Hall 305-962-0310
2
Facility Assistant Supervisor Kenneth Larkin 305-733-0104
3

Table 1. Mission Essential Functions

Parks & Recreation Divisions	Mission Essential Function	Priority for Declared Emergency
High Critical		
Administration	Answering & returning phone calls	
Administration	Scheduling of essential employees	
Adult Activity Center	Providing activities for 50+ population	
Adult Activity Center	Wellness checks for vulnerable populations	
Youth Center	Aftercare	
Youth Centers	Summer camp if applicable	
Medium Critical		
Administration	Administrative duties	
Administration	Scheduling updates	
Administration	Payroll	
Low Critical		
Administration	Attend monthly advisory board meetings	
Administration	Processing requisitions and Purchase Orders	
Administration	Paying of vendors	
Administration / Parks	Service playgrounds and safety inspections	
Administration / SE	Coordinate citywide events (special events)	
Special Events	Permit events & photo shoots	
Youth Center	Rental of pavilions and parks	
AAC / Tennis / YC / VP	Schedule programs & activities	
AAC / Tennis / YC / VP	Class offerings for the community (including youth, adult, senior)	
AAC / Tennis / YC / VP	Rental of facility (done at each center for that center)	
AAC	Specialized senior programming	
Not Rated		
Parks	Open secured parks	
Parks	Maintain Golf Course	
Parks	Sports fields in safe playable conditions	

Mission Essential Functions

The Community Recreation Department's primary function is to provide the City of Coral Gables residents and guests of all ages access to open space, facilities, programs and events to promote play, health and quality of life.

During a natural disaster or hurricane the primary functions of the Department shift to identify the essential functions for the safety and well-being of the community.

Table 1 provides a list of those essential functions, sorted by priority and by Division.

Community Recreation: Parks Inventory

Park	Address	Ball Field	Basketball	Benches	Bicycle Rack	Community Center	Drinking Fountain	Fitness Equipment	Golf Course	Parking	Pavilion	Pet-Friendly	Picnic Tables	Playground	Rental Available	Restrooms	Swimming	Tennis	Walking Path	Water Feature	Scenic Views
Coral Gables Adult Activity Center	2 Andalusia Avenue					●	●			●						●					●
Alcazar Plaza	700 Alcazar Avenue																				●
Balboa Plaza	2405 De Soto Blvd.			●								●								●	●
Betsy Adams and the Coral Gables Garden Club Park	4650 Alhambra Circle			●			●					●	●	●					●		●
Blue Road Open Space	757 Blue Road																				●
Carlos S. Kakouris Park	4935 Campo Sano Court			●																	●
Cartagena Park	401 Sunset Drive																				●
Catalonia Park	807 Catalonia Avenue																				●
City of Coral Gables Biltmore Golf Course	1210 Anastasia Avenue			●	●		●		●	●						●			●		●
Coral Bay Park	1590 Campamento Avenue		●	●	●		●			●	●		●	●					●		●
Coral Gables War Memorial Youth Center	405 University Drive	●	●	●	●	●	●	●		●	●		●	●	●	●			●		●
Country Club Prado	Country Club Prado											●								●	●
Durango Park	3405 Durango Street			●																	●
Enrique “Henry” Cepero Memorial Park	4600 San Amaro Drive																				●
Fred B. Hartnett Ponce Circle Park	2810 Ponce de Leon Blvd.			●	●					●		●							●	●	●
Freedom Plaza	981 E Ponce De Leon Blvd.									●											●
Granada Golf Course	2001 Granada Blvd.			●	●		●		●	●			●			●			●		●
Granada Park	5151 Granada Blvd.																		●		●
Ingraham Park	4751 West Ingraham Terr.			●	●		●	●		●		●	●						●	●	●
J. Fritz and Frances Gordon Park	800 Country Club Prado									●		●							●		●
Jaycee Park	1230 Hardee Rd.		●	●	●		●			●	●		●	●	●			●	●		●
Leucadendra Drive Triangle	331 Leucadendra Drive																				●
Lisbon Park	1015 Lisbon Street			●	●		●												●	●	●
Lola B. Walker Pioneers' Park	200 Grand Avenue																		●		●
Loretta Sheehy Park	410 Sunset Drive																				●
MacFarlane Linear Park	100 South Dixie Highway																		●		●
Maggiore Park	5028 Maggiore Street																		●		●
Majorca Park (Corner of Majorca & Granada)	937 Majorca Avenue																				●
Mall Street Median	Mall Street																				●
Marlin Park (Corner of Marlin & Bonito)	6540 Marlin Drive																				●
Merrick Park	400 Biltmore Way			●						●			●								●
Miss Lamar Louise Curry Park	2665 De Soto Boulevard																				●
Nellie B. Moore Park	202 Jefferson Dr.			●															●		●
Orduna Dr-Miller Rd Triangle Park	Corner of Orduna & Miller Road																				●
Phillips Park	90 Menores Avenue	●	●	●	●		●			●	●		●	●	●	●		●	●		●
Pierce Park	101 Oak Avenue			●			●				●		●	●	●						●
Pittman Park	115 Merrick Way			●						●									●	●	●
Ponce de Leon Park	1201 Ponce de Leon Blvd.			●						●									●	●	●
Robert J. Fewell Park	950 Coral Way			●	●														●		●
Rotary Centennial Park	512 Ponce De Leon Blvd.			●						●				●					●		●
Ruth Bryan Owen Waterway Park	3940 Granada Blvd.			●									●						●		●
Salvadore Park	1120 Andalusia Avenue	●	●	●	●		●			●	●		●	●	●	●		●	●		●
Salvadore Park Tennis Center	1120 Andalusia Avenue				●		●			●			●			●		●			●
San Benito Green	5750 Sunset Drive																				●
San Sebastian Park	130 San Sebastian Avenue																				●
Sarto Green	241 Sarto Avenue																				●
Sunrise Harbor Park	25 Sunrise Avenue		●	●	●		●			●	●		●	●	●				●		●
Tiziano Park	7700 Old Cutler Rd.																				●
Venetia Park	1047 Venetia Avenue																				●
Venetian Pool	2701 De Soto Blvd.			●	●		●			●			●		●	●	●		●	●	●
William A. Cooper Park	4920 Washington Dr.			●															●		●
William H. Kerdyk Biltmore Tennis Center	1150 Anastasia Avenue			●	●		●			●			●			●		●			●
William H. Kerdyk, Jr., and Family Park	6611 Yumuri Street			●	●		●	●		●	●	●	●	●					●		●
Young Park	950 Castile Plaza			●								●							●		●

Granada Golf Course & Parks: 2001 Granada Boulevard

Preparations While Operational: Pre-Storm Preparations 72-48 Hours

1. The Golf & Parks Superintendent & Assistant Superintendent will be responsible for securing the following items when a storm is approaching:
    - □ Trim trees
    - □ Fuel Diesel Tank
    - □ Fuel External Gas Tanks
    - □ 6 Chainsaws
    - □ Small generator
    - □ Large plastic bags
    - □ 10 flashlights and batteries
    - □ 50 feet of rope
    - □ 5 rolls of packing and masking tape
    - □ 3 rolls of visqeen plastic
    - □ 20 Sand bags

Pre-Storm Checklist: Hurricane Watch 48-36 hours

The Golf & Parks Superintendent and Assistant Superintendent and all Maintenance staff will be responsible for securing the following items when a storm is approaching:

1. Granada Golf Course
    - □ Remove all loose equipment such as flags, wastebaskets, portable benches, ball washers, water coolers, ect, and store them in the maintenance facility.
    - □ Install shutters around the Golf Pro Shop and adjacent restaurant.
    - □ Fuel up and service all motorized vehicles and equipment. Store as much equipment as possible inside maintenance building.
    - □ Fuel Diesel tank.
    - □ Prepare back-up generator
    - □ Power down all computers and unplug. Turn off electricity to the field satellites and the pump station.
    - □ Pick up any loose debris on the golf course.
    - □ Prepare hurricane supplies for clean-up such as; work gloves, eye protection, first aid supplies, flashlights, batteries, chainsaws, gas, ect.
    - □ Sandbag all entrances to prevent flooding of Maintenance Barn
2. Youth Center and Phillips Park Athletic Fields
    - □ Remove all loose equipment such as soccer goals, garbage cans, ect.
    - □ Turn off power to irrigation pumps and clocks.
3. All Playground Parks
    - □ Remove all loose equipment such as garbage cans, park benches, ect.
    - □ Turn off power to irrigation systems.
    - □ Take down all playground shade cloths
    - □ Check all parks for loose debris.

4. Salvadore and Biltmore Tennis Courts
    - Assist in removal and tie-down of wind screens.

Post-Storm Checklist: Post-Landfall 0-24 hours

1. When the storm has passed and/or power is restored all essential employees must report for assessment, cleanup and restoration of the facility
    A. The following employees will report to prepare facility for opening
        - Golf & Parks Superintendent
        - Golf & Parks Assistant Superintendent
        - Irrigation Foreman
        - Mechanic
        - Parks Foreman
        - And all Maintenance Staff
2. All employees shall check in on the employee call line as given by the City Of Coral Gables. Golf Course and Park Maintenance employees shall attempt to contact supervisor.
3. Prepare Maintenance Barn for staging area of staff to include set up of generator, powering on of ice machine and water fountain.
4. Make available use of showers and bathroom facilities for Rescue Recon personnel and staff as needed.
5. Supervisor shall assess damage to facilities and schedule clean-up duties as required.
6. All irrigation satellites shall be checked for damage before powering up.
7. After the hurricane, employees shall return all equipment to the golf course and parks. The shutters shall be removed from the Granada Pro Shop and restaurant and stored in the maintenance building.
8. Assist in the replacement of wind screens at tennis facilities.

Adult Activity Center: 2 Andalusia Avenue

Preparations While Operational: Pre-Storm Preparations 72-48 Hours

1. The Adult Activity Center Supervisors and Maintenance Worker will be responsible for securing the following items when a storm is approaching:
   - □ Large plastic bags
   - □ 10 flashlights and batteries
   - □ 5 rolls of packing and masking tape
   - □ 4 rolls of plastic sheeting
   - □ Large packing boxes
   - □ 14 Large sandbags
   - □ 15 gallons of bottled water

Pre-Storm Checklist: Hurricane Watch 48-36 hours

1. All staff will prepare the facility as follows:
   - A. Main Lobby
     - □ Move all furniture away from doors and windows.
     - □ Clear all surfaces of loose items. All documents are to be boxed, and other items are to be put in a storage closet.
     - □ Sandbag exterior of main entrance doors
     - □ Lock and seal doors with plastic sheeting
     - □ Unplug all electronics
     - □ Cover TV, computers, and wire with plastic sheeting.
     - □ Remove and store all artwork, plants, magazine racks, and decorations
   - B. Registration Lobby
     - □ Clear surface of Credenza
     - □ Clear all fliers and registration documents
     - □ Lock items in credenza
     - □ Cover credenza and table with plastic sheeting
   - C. Registration Office
     - □ Cover computers, desk, file cabinets and cash registers with plastic sheeting
     - □ Place all paper and books in cabinets and closets
     - □ Move all objects such as tape dispensers and staplers into desks
     - □ Remove pictures on walls and store in closets
     - □ Lock doors and check windows
     - □ Unplug all electrical equipment, copy machine, etc. and cover with plastic sheeting
   - D. Office 1 & 2
     - □ Move all books and papers away from windows and cover with plastic sheeting
     - □ Unplug all electrical appliances and machines. Cover or put in safe place

- □ Cover all file cabinets, desks, computers, bookcases with plastic sheeting
- □ Take all pictures, trophies, etc. off walls and put in safe place
- □ Move all heavy objects off desk tops and secure
- □ Make sure all computer data files are backed up
- □ Move any valuable/sensitive materials into safes
- □ Lock doors

E. Classroom #1, #2, & #3

- □ Cover tables with plastic sheeting
- □ Unplug, cover and move electrical powered games, TV's and computers away from windows
- □ Cover chairs and tables with plastic sheeting
- □ Lock all doors and check windows
- □ Clear counter tops
- □ Move any loose items into the supply closets in Classroom #3
- □ Plug classroom #3 sink, and fill with water
- □ Lock doors

F. Conference Room

- □ Remove and secure all wires connected to Conference Table.
- □ Cover TV and all electronics with plastic sheeting
- □ Remove any electronic equipment off of the floor
- □ Cover table, chairs, and credenza with plastic sheeting
- □ Lock all loose items in credenza
- □ Lock door

G. Media Library

- □ Move laptop computers, wires, and small electronic into the drawers and lock.
- □ Cover TV and printer with plastic sheeting
- □ Cover tables and chairs with plastic sheeting
- □ Cover shelves/drawers with plastic sheeting
- □ Lock door

H. West Corridor (Restroom Hallway)

- □ Remove art work and move to Maintenance closet
- □ Unplug water dispenser, secure wire, and move to registration office
- □ Power off both elevator lift (Switch inside service door)

I. Central Corridor

- □ Remove and store all artwork and plants in Main storage/Maintenance closet

J. IT Closet

- □ Power off and unplug all electronics
- □ Cover all equipment and wiring with plastic sheeting
- □ Sandbag exterior of doors

K. East Corridor

- □ Power off both elevator lift (Switch inside service door)

L. East Lobby

- □ Move all furniture away from doors and windows.
- □ Clear all surfaces of loose items. All documents are to be boxed, and other items are to be put in a storage closet.
- □ Sandbag exterior of lobby entrance doors
- □ Lock and seal doors with plastic sheeting
- □ Unplug all electronics
- □ Cover TV and wires with plastic sheeting.
- □ Remove and store all artwork, plants, magazine racks, and decorations

M. Multipurpose room

- □ Move supply rack to Main storage closet
- □ Lower window blinds
- □ Remove all artwork and store in main storage
- □ Sand bag the street door

N. Main Storage/Maintenance office

- □ Cover A/V Equipment with plastic sheeting
- □ Make clear pathway to access any essential items (Tools, tape, batteries, etc.).

O. Kitchen

- □ Put all materials in cabinets or storage closet
- □ Place all heavy objects in storage closet
- □ Lock all doors and check windows
- □ Cover stove, and oven with plastic sheeting
- □ Move the microwave to the kitchen storage closet
- □ Close and secure the service windows

Rescue Recon Prep Checklist: HURRICANE WARNING 36-24 Hours

1. When the Adult Activity Center becomes activated as a Rescue/Recon Shelter the following will occur:

A. The following staff will be alerted that the Adult Activity Center will be activated and to prepare to be on duty as facility hosts. The following staff will be needed:

- □ Adult Activity Supervisor
- □ Asst. Adult Activity Supervisor
- □ 1 Maintenance Staff

B. Prepare signs for status of facility closure

C. Prepare Multipurpose Room

- □ 60 chairs
- □ 4- 6' Round tables
- □ 2- 8' Rectangular tables
- □ Disposable Table Cloths
- □ Extension cords
- □ Coffee Machines
- □ Serving Utensils/Trays

- □ Sleeping Cots
- □ Manual Air Pumps
- □ Blankets
- □ Paper Cups
- □ Heavy Duty Trash bags
- □ 4- Large Trash Bins
- □ Batteries
- □ Battery-Operated Radio
- □ Flashlights & Lanterns
- □ Lighters & Matches
- □ Signage
- □ Tape
- □ Walkie-Talkies
- □ Portable AC unit
- □ Facility Storm Manuals

D. Prepare Kitchen

- □ 6’ rectangular table
- □ cooler with ice
- □ All food items from the hurricane storage
- □ Bottled water
- □ Cups, plates, napkins, and utensils
- □ Serving Supplies & Utensils (Bowls, trays, napkin/utensil holders, etc.)
- □ Gas camping stove
- □ Propane
- □ Large Coffee Machine
- □ Coffee Dispensers
- □ Coffee & Tea Supplies (Coffee, filters, creamer [powder], sweeteners, etc.)
- □ Can Openers
- □ Gloves

E. Prepare Conference Room

- □ TV
- □ Phone
- □ Coffee Station

F. General Preparations

- □ Make sure all essential supplies are on hand – paper goods, bathroom essentials, etc.

Post-Storm Checklist: Post-Landfall 0-24 hours

1. When the storm has passed and/or power is restored all essential employees must report for assessment, cleanup and restoration of the facility

B. The following employees will report to prepare facility for opening

- □ Adult Activity Supervisor

- Assistant Adult Activity Supervisor

- All Guest Service Specialists
- All Maintenance Personnel

C. All unused materials and supplies to be stored in hurricane storage room
D. All trash, tree branches and debris to be removed from all walkways, entrances and open areas
E. Staff to give a written assessment of damage

Venetian Pool: 2701 DeSoto Boulevard

Preparations While Operational: Pre-Storm Preparations 72-48 Hours

- □ Secure portion of Lifejackets and Bins in Classrooms
- □ Secure Portion of Lounge Chairs in Classrooms
- □ Contact Public Works for sandbags and prepare Sandbags
- □ Tie up and loose blinds in the towers to prevent crashing against windows

Pre-Storm Checklist: Hurricane Watch 48-36 hours

1. The Venetian Pool Supervisors and Maintenance Worker will be responsible for securing the following items when a storm is approaching:
    - □ Toss all facility anti-slip matts into the water
    - □ Forward calls to City emergency hotline number
    - □ Post Facility Signage that the Venetian Pool will be closed until further notice. We Apologize for the inconvenience. Update Website and Social Media
    - □ Drain Pool 3 Feet
    - □ Flip Benches over & Bring in Free standing signs
    - □ Secure Lifejackets and bins in classrooms
    - □ Bring in Trash Cans
    - □ Sandbag the entrances
    - □ Secure Pool lines and buoys
    - □ Move all computers and electronic equipment away from windows and store in waterproof container in closet.
    - □ Grab Rope and Secure Upper Patio Chandelier to railings. Prevent swinging.
    - □ Secure Lounge Chairs into Beach classroom.
    - □ Remove Clock by Handicap Elevator.
    - □ Bring all tables, chairs, umbrellas, and bases into the concessions and classrooms.
    - □ Tie up any loose awnings in the Towers
    - □ DRAIN the pool between 2-3 feet.
    - □ Take pictures and document prior to storm and post-storm facility conditions.
        - o Save them to the Supervisor Drive Prior to the storm.
    - □ TURN off breakers to the pumps.
    - □ LOCK DOORS AND GATES OF FACILITY

Post-Storm Checklist: Post-Landfall 0-24 hours

1. When the storm has passed and/or power is restored all essential employees must report for assessment, cleanup and restoration of the facility
    - A. The following employees will report to prepare facility for opening
        - □ Venetian Pool Supervisor
        - □ Assistant Venetian Pool Supervisors

- □ Maintenance Worker II
- □ All Guest Service Specialists
- □ All Lifeguards

B. The following steps should be completed post storm when the all clear has been given to safely enter the facility

- □ Drive perimeter looking for down electric-wires or anything potentially hazardous prior to getting on foot and entering the building.
- □ Call FPL to report electric outage/ down wires.
- □ Document/ take pictures of facility damage prior to setting up tables, chairs, matts, etc.
- □ Post Facility Signage that the Venetian Pool will be closed until further notice. We apologize for the inconvenience. Update Website and Social Media
- □ Call in additional staff to set up patio areas and get remove branches/ foliage
- □ Toss any food that has been thawed. Inspect staff and concession fridges and food.
- □ Look for signs of pests.
- □ Once electricity is back: start the drain cycle and clean pool floor
- □ Call Dept. Director to send surplus staff to other divisions/ departments if needed.

War Memorial Youth Center: 405 University Drive

Preparations While Operational: Pre-Storm Preparations 72-48 Hours

2. The Youth Center Supervisor and Maintenance Foreman will be responsible for securing the following items when a storm is approaching:
   - □ Large plastic bags
   - □ 10 flashlights and batteries
   - □ 50 feet of rope
   - □ 5 rolls of packing and masking tape
   - □ 3 rolls of visqeen plastic
   - □ Large packing boxes
   - □ 15 gallons of bottled water

Pre-Storm Checklist: Hurricane Watch 48-36 hours

1. All staff will prepare the facility as follows:

   A. Main Office (First Floor)
   - □ Cover computers, typewriters, desk, file cabinets and cash registers with visqueen
   - □ Place all paper and books in cabinets and closets
   - □ Move all objects such as tape dispensers and staplers into desks
   - □ Remove pictures on walls and store in closets
   - □ Lock doors and check windows
   - □ Unplug all electrical equipment, copy machine, etc. and cover with visqueen

   B. Administrative Offices (Second Floor)
   - □ Move all books and papers away from windows and cover with visqueen
   - □ Unplug all electrical appliances and machines. Cover or put in safe place
   - □ Cover all file cabinets, desks, computers, bookcases with visqeen
   - □ Take all pictures, trophies, etc. off walls and put in safe place
   - □ Move all heavy objects off desk tops and secure
   - □ Move any plants away from windows
   - □ Make sure all computer data files are backed up

   C. Teen, Activity and Toddler room
   - □ Cover game tables with visqeen
   - □ Unplug, cover and move electrical powered games, TV's and computers away from windows
   - □ Cover chairs and tables with visqueen
   - □ Lock all doors and check windows
   - □ Clear counter tops

   D. Gymnasium
   - □ Place floor covering over entire gym
   - □ Secure floor covering with tape

   E. Halls and Patios
   - □ Place all patio furniture in Theater

- □ Move all exterior trash cans into Theater. Provide trash bags in bottom of trash cans
- □ Make sure there is no lawn equipment or any other material left anywhere on the grounds
- □ Move all tables and chairs into Theater
- □ Move any recreational equipment into Theater

F. Ceramics Room
- □ Put all clay molds on floor or in the closet
- □ Unplug and cover potter wheels with visqueen.
- □ Lock all doors and check windows
- □ Place all heavy objects on floor and clear counters
- □ Move all toxic and flammable materials to a safe place

G. Playground
- □ Tie swing chains and seats securely to post

H. Theater
- □ Place all chairs and tables in storage closet
- □ Lock all doors

I. Gymnastics Gym
- □ Secure all movable gymnastics equipment
- □ Lock all doors

J. Discovery Playground
- □ Place pit balls in bag and store in maintenance room

K. Arts and Crafts Room
- □ Put all materials in closet
- □ Place all heavy objects on floor
- □ Lock all doors and check windows

L. Vestibule
- □ Remove all items from check in center and store in front office
- □ Move furniture from waiting area on second floor and store in recreation staff offices
- □ Lock all doors and check windows

M. Catering and Teaching Kitchen
- □ Clean and organize for use as a shelter kitchen
- □ Inspect all appliances to ensure they function properly. Repair as needed
- □ Empty and clean all refrigerators

N. Fitness Center
- □ Secure all equipment
- □ Lock all doors

O. Maintenance Area
- □ Ensure all trash bins have been emptied and make sure area is clear

P. Field House, Equipment and Athletic Storage Rooms and Concession Stand
- □ Make sure all equipment is secure
- □ Unplug all electrical devices
- □ Lock all doors and windows

2. Vehicles

    A. Assure that all gas tanks are filled in truck and vans and park vehicles in a safe place away from trees

3. Shutter Installation
    A. Maintenance Foreman will coordinate the installation of storm shutters with Public Works and teams will be formed to complete the installation
        - □ 2 staff inside storage room
        - □ 2 staff moving shutters
        - □ 6 staff installing inside facility
        - □ 7 staff installing outside
4. General Safeguards for the entire facility
    - □ Check grounds for any loose equipment or debris
    - □ Shut off lights and unplug all electrical equipment
    - □ Lock all doors
    - □ Close all windows
    - □ Lock all gates in the breezeway and field
    - □ Secure all athletic equipment located on the field

Post-Storm Checklist: Post-Landfall 0-24 hours

1. The Youth Center Supervisor, Maintenance Foreman and essential staff will be responsible for inspecting facility and completing damage assessment.
2. All debris and branches will be cleared from walkways and entrances.
3. Maintenance staff will begin removal of shutters to facilitate access for post storm/hurricane procedures.
4. All staff will report to work as scheduled and prepare the facility as follows:
    A. Main Office (First Floor)
        - □ Remove covers from computers, typewriters, desk, file cabinets and cash registers with visqueen
        - □ Re-organize all stored office supplies.
        - □ Place all pictures on walls.
        - □ Lock doors and check windows
        - □ Reconnect all electrical equipment, copy machine, etc.

    B. Administrative Offices (Second Floor)
        - □ Move all books and papers away from windows and cover with visqueen
        - □ Reconnect all electrical appliances and machines.
        - □ Restore all file cabinets, desks, computers, bookcases w
        - □ Place all pictures, trophies, etc. on walls.

    C. Teen, Activity and Toddler room
        - □ Uncover game tables and furniture.
        - □ Reconnect and place electrical powered games, TV’s and computers.

    D. Gymnasium
        - □ Remove and store floor covering.

    E. Halls and Patios
        - □ Place all patio furniture in its designated location.

- □ Place all exterior trash cans in their designated locations.

F. Ceramics Room
- □ Place all equipment and materials in designated areas.
- □ Uncover and reconnect all TVs and electronics.

G. Playground
- □ Remove all debris and prepare equipment for public use.

H. Theater
- □ Take all equipment and furniture back to their designated areas.

I. Gymnastics Gym
- □ Place all gymnastics equipment back in their designated areas.
- □ Reconnect and uncover all office supplies.

J. Discovery Playground
- □ Clear area of debris and prepare for public use.

K. Arts and Crafts Room
- □ Place all equipment back in its designated area.
- □ Reconnect and uncover all electronics.

L. Vestibule
- □ Check area for debris and water damage.
- □ Move furniture back from waiting area on second floor.
- □ Reconnect and uncover all monitors, phones, computers etc.

M. Catering and Teaching Kitchen
- □ Inspect all appliances to ensure they function properly. Repair as needed

N. Fitness Center
- □ Place all equipment back in its designated area.
- □ Reconnect and uncover all electronics.

O. Maintenance Area
- □ Ensure all trash bins have been emptied and make sure area is clear

P. Field House, Equipment and Athletic Storage Rooms and Concession Stand
- □ Make sure all equipment is secure
- □ Reconnect all electrical devices

Q. General Safeguards for the entire facility
- □ Check grounds for any loose equipment or debris
- □ Check all electrical equipment

5. Vehicles
   - □ Assure that all vehicles are brought back to facility from parking areas.
6. Shutter Removal
   - □ Maintenance Foreman will coordinate the removal of storm shutters with Public Works and teams will be formed to complete the removal
     - □ 2 staff inside storage room
     - □ 2 staff moving shutters
     - □ 6 staff removing inside facility
     - □ 7 staff removing outside facility

Salvadore Tennis Center: 1121 Andalusia Avenue

William H. Kerdyk Biltmore Tennis Center: 1150 Anastasia Avenue

Preparations While Operational: Pre-Storm Preparations 72-48 Hours

1. The Tennis Supervisor and Assistant Supervisor will be responsible for securing the following items when a storm is approaching:
   - □ Large plastic bags
   - □ 50 feet of rope
   - □ 5 rolls of packing and masking tape
   - □ 3 rolls of visqeen plastic
   - □ Plastic containers
   - □ 10 filled sandbags

Pre-Storm Checklist: Hurricane Watch 48-36 hours

1. All Part-Time and full time staff must report to secure both tennis facilities
2. All staff will prepare the facility as follows:

   A. Drop windscreens on all fences
   - □ Cut three sides of the cable ties (two sides and the top)
   - □ Roll the bottom of the windscreen into a tight roll
   - □ Tie wind screen to fence with strong rope in three places evenly spaced apart (approximate time is 14+ Man hours)
   - □ Remove signage from fences that could become projectiles in strong winds. Store in maintenance closet.
   - □ Wind screens might need to be dropped and tied down prior to the City Manager's office making the call. It is difficult to drop wind screens when the wind is in excess of 20 to 25 MPH.

   B. Put the following items into the storage rooms/pro-shop (Biltmore)/restrooms:
   - □ Teaching carts
   - □ Tidi-court baskets
   - □ Roll-Dri's
   - □ Line sweepers
   - □ Drag brooms
   - □ Plastic trash cans
   - □ 90 gallon Waste Management trash cans
   - □ Tennie two step shoe cleaners
   - □ Outdoor patio furniture
   - □ Outdoor patio cushions
   - □ If there is not enough room in the restrooms then tie each one individually to the fence and tie down the lid so trash will not blow out

   C. Take golf cart to Granada Golf Course cart barn

   D. Tie ALL picnic tables, benches and utility cart to the fence or railings

   E. Pro Shop:
   - □ Put CPU and printer in North storage room

- □ Cover with 50-60 gallon plastic bags all electronic items

F. Check entire facility inside fence, building and park for any loose items
G. Change out-going message on telephone about the impending storm
H. Turn the timer off for the irrigation system for the clay courts
I. Do not turn the alarm on when closing the Pro-Shop
J. Put all important documents in a plastic bag in the North storage room
K. Wrap flag pole halyard around pole and secure to the cleat
L. Lock all gates securely with no play in the chain
M. Lock Pro-Shop door
N. Tape the Pro-Shop door seams with painters tape to keep rain water out
O. Place filled sand bags at entrance of pro-shop to keep any floodwater out.
P. Tape the North storage room door seams with painters tape to keep rain water out

Post-Storm Checklist: Post-Landfall 0-24 hours

1. When the storm has passed and/or power is restored all essential employees must report for assessment, cleanup and restoration of the facility

A. The following employees will report to prepare facility for opening
   - □ Tennis Supervisor
   - □ Assistant Tennis Supervisor
   - □ Maintenance Worker
   - □ All Guest Service Specialists

B. All Part-Time and Full time staff must report to both tennis facilities
C. Assess and document damage in writing and with photos
D. Email Assistant Director, Director, and Public Works notice and documentation of any damage
E. Raise windscreens on all fences
   - □ Un-tie wind screens from fences
   - □ Use zip ties to re-attach wind screens to the top and sides of each fence section
   - □ Use zip ties to re-attach signage to the fences
   - □ Requires crew of 10 people 8+ man hours

F. Return the following items stored into the restrooms to their regular locations:
   - □ Teaching carts
   - □ Tidi-court baskets
   - □ Roll-Dri's
   - □ Line sweepers
   - □ Drag brooms
   - □ Plastic trash cans
   - □ 90 gallon Waste Management trash cans
   - □ Tennie two step shoe cleaners
   - □ Outdoor patio furniture
   - □ Outdoor patio cushions

□ Un-tie anything tied to the fences

G. Retrieve the golf cart from the Granada Golf Course cart barn and return to storage area adjacent to court 5

H. Un-tie all picnic tables, benches and utility carts from the fences or railings

I. Pro Shop:

   □ Retrieve CPU, fax machine and printer from North storage room and return to office

   □ Return all electronic items from North storage room

   □ Return all important documents from the North storage room

J. Change out-going message on telephone back to regular message

K. Turn the timer on for the irrigation system for the clay courts

L. Un-wrap flag pole halyard around pole and raise flags

M. Un-lock all gates, as needed

City of Coral Gables

COMMUNITY RECREATION

Emergency Supply Bag

Inventory of Items:

□ Multi tool

□ First aid kit

□ Waterproof backpack with laptop/documents compartment.

□ Emergency radio with solar/crank power, USB charger, and light.

□ Crank/solar-powered flashlight

□ Waterproof documents cover/pack

□ Portable USB drive (flash drive or hard drive) for files storage/backup

□ Emergency portable snacks

□ Breathing masks

□ Mosquito repellent

□ Sunscreen

□ Waterproof cover for documents

□ Waterproof cell phone functional cover

□ Water packs for 72 hours

Community Recreation - Parks & Recreation

Vital Records List

6000 - Administration

- Contracts
- Employee Evaluations
- Employee Files
- Maps & Site Plans
- Marketing/Branding Files
- Monthly & Annual Reports
- MOU Agreements
- NRPA Accreditation Documents (10 Binders)
- Payroll Back-up

6010 - Salvadore & Biltmore Tennis Center

- Accident/Incident Back-Up Documents
- Commission Reports
- Court Reservation Books
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Financial Back-up Documents
- Invoicing Back-up Documents
- Monthly & Annual Reports
- Payroll Back-up
- P-Card Back-up Documents
- Petty Cash Back-Up
- Refund Back-Up Documents
- Registration Forms
- Tennis Professional Contractor Agreements
- Tennis Professional Contractor Reconciles
- Work schedules

6020 - Venetian Pool

- Accident/Incident Back-Up Documents
- Concessions Operational License
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Employee Schedules
- Facility Rental Documents
- Financial Back-up Documents
- In-Service Training Records
- Invoicing Back-up Documents
- Jeff Ellis & Associates Audit Documents
- Lifeguard Licenses
- Monthly & Annual Reports
- Payroll Back-up
- P-Card Back-up Documents
- Petty Cash Back-Up
- Pool Operational License (CPO)
- Chemical Safety Data Sheets
- Pool Permit
- Quarterly Water Quality Lab Tests
- Refund Back-Up Documents
- Registration forms
- Rescue Reports
- Vendor Contracts
- Volunteer Files

6050 - Youth Center

- Accident/Incident Back-Up Documents
- Concession operational License
- Contractor Reconcile Back-Up Documents
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Employee Schedules
- Facility Rental Documents
- Financial Back-up Documents
- Invoicing Back-up Documents
- Monthly & Annual Reports
- Payroll Back-up

- P-Card Back-up Documents
- Petty Cash Back-Up
- Referee Receipts
- Refund Back-Up
- Registration forms
- Vendor Contracts
- Volunteer Files

6060 - Adult Activity Center:

- Accident/Incident Back-Up Documents
- Certificate of Occupancy
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Employee Schedules
- Financial Back-up Documents
- Fire Inspection
- Invoicing Back-up Documents
- Monthly & Annual Reports
- Payroll Back-up
- P-Card Back-up Documents
- P-Card Files
- Petty Cash Back-Up
- Refund Back-Up
- Registration forms
- Vendor Contracts
- Volunteer Files

6065 – Special Events:

- Community Service Booth Applications
- Contact forms from the HOA’s
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Employee Schedules
- Event Site Maps
- Farmer’s Market Cookbook
- Farmer’s Market Vendor Applications
- Financial Back-up Documents
- Food Manager’s License & Documents
- Invoicing Back-up Documents
- Monthly & Annual Reports
- Payroll Back-up
- P-Card Back-up Documents
- Photo/Video Permits
- Special Event Calendar of Events
- Special Event Permits
- Vendor Agreements
- Volunteer/Intern Files

6070 – Golf & Parks:

- Accident/Incident Back-Up Documents
- Employee Evaluations
- Employee Files
- Employee Manuals & Procedures
- Employee Schedules
- In-Service Training Records
- Invoicing Back-up Documents
- Material Safety Data Sheets
- Monthly & Annual Reports
- Operational License
- Payroll Back-up
- P-Card Back-up Documents
- Site Plans
- Water Quality Lab Tests

PCI DSS Requirement		Expected Testing	Response ♦ (Check one response for each requirement)				
			In Place	In Place with CCW	Not Applicable	Not Tested	Not in Place
12.10 Suspected and confirmed security incidents that could impact the CDE are responded to immediately.							
12.10.1	An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident. The plan includes, but is not limited to: • Roles, responsibilities, and communication and contact strategies in the event of a suspected or confirmed security incident, including notification of payment brands and acquirers, at a minimum. • Incident response procedures with specific containment and mitigation activities for different types of incidents. • Business recovery and continuity procedures. • Data backup processes. • Analysis of legal requirements for reporting compromises. • Coverage and responses of all critical system components. • Reference or inclusion of incident response procedures from the payment brands.	• Examine the incident response plan. • Interview personnel. • Examine documentation from previously reported incidents.	☒	□	□	□	□
12.10.2	At least once every 12 months, the security incident response plan is: • Reviewed and the content is updated as needed. • Tested, including all elements listed in Requirement 12.10.1.	• Interview personnel. • Examine documentation.	☒	□	□	□	□
12.10.3	Specific personnel are designated to be available on a 24/7 basis to respond to suspected or confirmed security incidents.	• Interview responsible personnel. • Examine documentation.	☒	□	□	□	□
12.10.4	Personnel responsible for responding to suspected and confirmed security incidents are appropriately and periodically trained on their incident response responsibilities.	• Interview incident response personnel. • Examine training documentation.	☒	□	□	□	□

City of Coral Gables - Community Recreation
All Full Time Staff - Annual Meeting Agenda
Friday, December 13, 2024, from 8:30 a.m. to 2:00 p.m.

Time:	Topic:	Speaker:
8:00 a.m.	Breakfast social	All
8:30 a.m.	Welcome & Accomplishments & Service Pins	Fred
9:00 a.m.	Community Recreation Business Plan & Recreation Programming Plan: • Department Executive Summary & History - Carolina • Department History, Mission, Vision, Values & Goals - Sarah • City & Department Organizational Structure - Fred • Department Core Programs, Services & Facilities - Fred • Marketing Analysis: Segregation, Service Area, Competition & Trends - Fred • Department Operations Analysis: Expenses & Revenues, Operating Standards, CIP Needs and Strategic Plan - Carolina • Department Implementation Strategies: Marketing, Branding, Pricing Strategies & Organizational Needs – Fred	All
10:00 a.m.	Break	NA
10:15 a.m.	Leadership Workshop	Carolina
11:30 a.m.	Policies & Procedures, Employee Handbooks, Personnel Involvement City Safety Manual / General Security Plan / Risk Management Plan / Vehicle Safety / Playground Safety / Golf & Maintenance Safety / Emergency Procedures & Contact Flowchart / Workers Compensation	Carolina
12:00 p.m.	Lunch & Announcements	All
12:30 p.m.	Community Recreation Master Plan Update, ADA Transition Plan Update, Records Disaster Mitigation and Recovery Plan Update & Future Planning	Carolina
1:00 p.m.	Infor Presentation: Leave Request & Pay Stub	Sarah
1:10 p.m.	In-Service Trainings - Law Enforcement / Active Shooter	Carolina
1:30 p.m.	Customer Service Standards & Training	Carolina
1:50 p.m.	Work Environment & Ethics Training • Sexual Harassment • Gift Policy • Honor Code	Carolina
2:00 p.m.	Annual Picture, Feedback, Q&A & Closing	All

Annual Meeting Sign-In: Friday, December 13, 2024

Albritton, Frank ______________________________

Butler, John ______________________________

Cobarrubia, Edel ______________________________

Correa, Yonas ______________________________

Couceyro, Fred______________________________

Cruz, Jose______________________________

Diaz, Katherine ______________________________

Espino, Sarah ______________________________

Freeman, Leonard ______________________________

Galdamez, Jonathan ______________________________

Garcia, Valentin ______________________________

Garcia, Yesenia ______________________________

Gavarrete, Norma ______________________________

Gilman, Daren ______________________________

Gomez, Robert ______________________________

Guerrero, Manuel______________________________

Hannah, Ana ______________________________

Jacques, Jean ______________________________

Jones, Jerry ______________________________

Knight, Mark ______________________________

Hastings, Catie Caspian______________________________

Larkin, Kenneth ______________________________

Lainfiesta, Susan ______________________________

Laurenceau, Max “Kiki”______________________________

Llompart-Santi, Carlos ______________________________

Morcate, Marilyn ______________________________

Nuñez, Jose ______________________________

Pepin, Cassidy ______________________________

Pichardo, Carlos ______________________________

Pinion, Valerie ______________________________

Rocha, Michael ______________________________

Rodriguez, Fabio ______________________________

Rodriguez, Farah ______________________________

Rodriguez, Yanessa ______________________________

Vester, Carolina ______________________________

Vilar, Jose ______________________________

Warren, Roderick ______________________________

Walters, Gregory ______________________________

City of Coral Gables Community Recreation

Annual Strategic Meeting
December 2024

CORAL GABLES
THE CITY BEAUTIFUL

Agenda for the Day:

- Loyalty Recognition & Opening Remarks
- Department Accomplishments & Announcements
- Review Community Recreation Business Plan
- Leadership Workshop
- Policies & Procedures / Personnel Involvement
- Master Plan Update & Future Planning
- Timeclock/Payroll/Leave Request Transition with Infor
- Law Enforcement Training
- Customer Service Training
- Work Environment: Ethics, Sexual Harassment & Gift Policy

Susan Lainfiesta

For 10 Years of Service

CONGRATULATIONS

Farah Rodriguez

For 10 Years of Service

CONGRATULATIONS

Yanessa Rodriguez

For 10 Years of Service

CONGRATULATIONS

Leonard Freeman Jr.

For 20 Years of Service

CONGRATULATIONS

Carolina Vester

For 20 Years of Service

CONGRATULATIONS

Carlos Pichardo

For 25 Years of Service

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Served the community by providing recreational facilities and programs for all ages:

- Held several special events with a combined attendance of over 93,000 event participants.
- Granada Golf course continued to operate at near capacity with over 50,000 rounds of golf.
- The Granada Pro Shop was renovated and opened for operation.
- Continued to provide programming to adults through the Adult Activity Center. The center registered over 22,000 visits with over 9,000 different program registrations.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

- The Youth Center was a focal point of activity with an approximate 450,000 visits to the Youth Center facility, field and playground.
- There were over 13,000 individual program enrollments and approximately 35,000 fitness center visits.
- There were over 4,000 summer camp registrations.
- Venetian Pool continued to be a premier destination for visitors with over 55,000 visitors to the pool.
- The Country Club's athletic club and pool had over 50,000 visits. The Country Club also hosted over 150 revenue-driven events.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Further developed the Diversity, Equity and Inclusion services through the following programs, innovations, and initiatives:

- Received the National Inclusion Project Accreditation for City-run Camps and Programs at the Coral Gables War Memorial Youth Center.
- Introduced events to the DEI population that would coincide with larger city-wide events to provide a programming experience that would better serve this community.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Further developed the Diversity, Equity and Inclusion services through the following programs, innovations, and initiatives:

- Events included the Sensory Friendly 4th of July celebration at the Ruth Bryan Owen Waterway Park in conjunction with the larger A Gables Fourth celebration at the Biltmore Golf Course, Gentle Trick or Treat event in conjunction with the Youth Center eggstreme egg hunt, and the gentle Trick or Treat event to celebrate Halloween.
- Provided events to the community through partnerships including the International Cochlear Implants Day with the University of Miami and Battle of the Badges kickball game with city Police and Fire Departments.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Developed service innovations and resource additions that increased customer service, cost savings and quality of life goals.

- Completed the transition from gas blowers to electric blowers for maintenance tasks.
- Introduced the use of recycled mulch made within the city for use at playground parks.
- Installed 16 new dog waste stations to bring the total of dog waste stations maintained by the Department to over 145. Installed 4 new Little Libraries, 25 benches, 4 picnic tables, and 9 new memorial benches in parks.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Developed service innovations and resource additions that increased customer service, cost savings and quality of life goals.

- Installed new LED lighting in the Youth Center fitness center and the Granada Golf Course Pro Shop.
- Initiated several battery and recycling stations at Community Recreation facilities.
- Through a partnership with Doody Calls, the city received 40 new dog waste stations for the dog waste program.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Developed new program and event offerings that met resident's needs, increased customer satisfaction and advanced quality of life goals.

- Increased open play for pickleball and flamenco dance at the Youth Center, Tango classes, summer camp program and Holiday events such as Cars and Santa, 4th of July BBQ and Memorial Day Bash event at the Country Club, Fleet Week Naval Band Jazz Waves Concert at Venetian Pool, Halloween Spooktacular, Golden Egg Hunt, domino club, Zumba after hours and DYI jewelry making at the Adult Activity Center and the Funky Pickle Tournament with over 300 pickleball players at the Biltmore Tennis Center.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

The Community Recreation Department received accolades and recognitions this year including:

- The Department continued annual compliance with National Reaccreditation by the Commission of Accredited Parks and Recreation Agencies and has maintained National Accreditation for its 23rd year.
- Tennis Operations Supervisor Robert Gomez was awarded the USPTA Lifetime Achievement Award for his 30 years of service in tennis.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

The Community Recreation Department received accolades and recognitions this year including:

- The Venetian Pool was awarded the Jeff Ellis and Associates Gold Award for water safety. Venetian Pool also featured on FIFA World Cup 2026 Promotion.
- The Coral Gables Country Club Voted the Best Wedding Venue in Miami-Dade in Miami Herald’s Miami-Dade Favorites issue.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Assisted in the development and renovation of parks and facilities.

- Implemented multiple projects at Venetian Pool. The Pool resurfacing project was completed. The Concession stand construction is underway and scheduled for completion in 2024. Planning has begun for Structural repairs at the pool facility.
- Several construction and improvement projects were completed including the resurfacing of the clay courts at Salvadore Tennis Center, the Salvadore Dog Park, The Kid’s Lounge at the Coral Gables Country Club, the resurfacing of the youth center basketball courts for pickleball use and the exterior painting of the Youth Center building.

FISCAL YEAR 2024 ACCOMPLISHMENTS:

Assisted in the development and renovation of parks and facilities.

- Construction completed on the Granada Golf Course Pro Shop, construction on the Granada Diner project is underway and scheduled for completion in 2024.
- Completed the community input process and concept design process for several upcoming projects including Phillips Park, Blue Road Park, William Cooper Park, Nellie B. Moore Park, and Toledo and Alava Park.

Community Recreation Staff

Why Statement

Coral Gables
The City Beautiful

Do You Remember Our Why Statement?

Why do we come to work to do what we do each day?

“To enhance daily life so that we can inspire a sense of community”

City of Coral Gables
Community Recreation

2024 Business Plan & Department Review

Coral Gables®
The City Beautiful

Executive Summary

Executive Summary

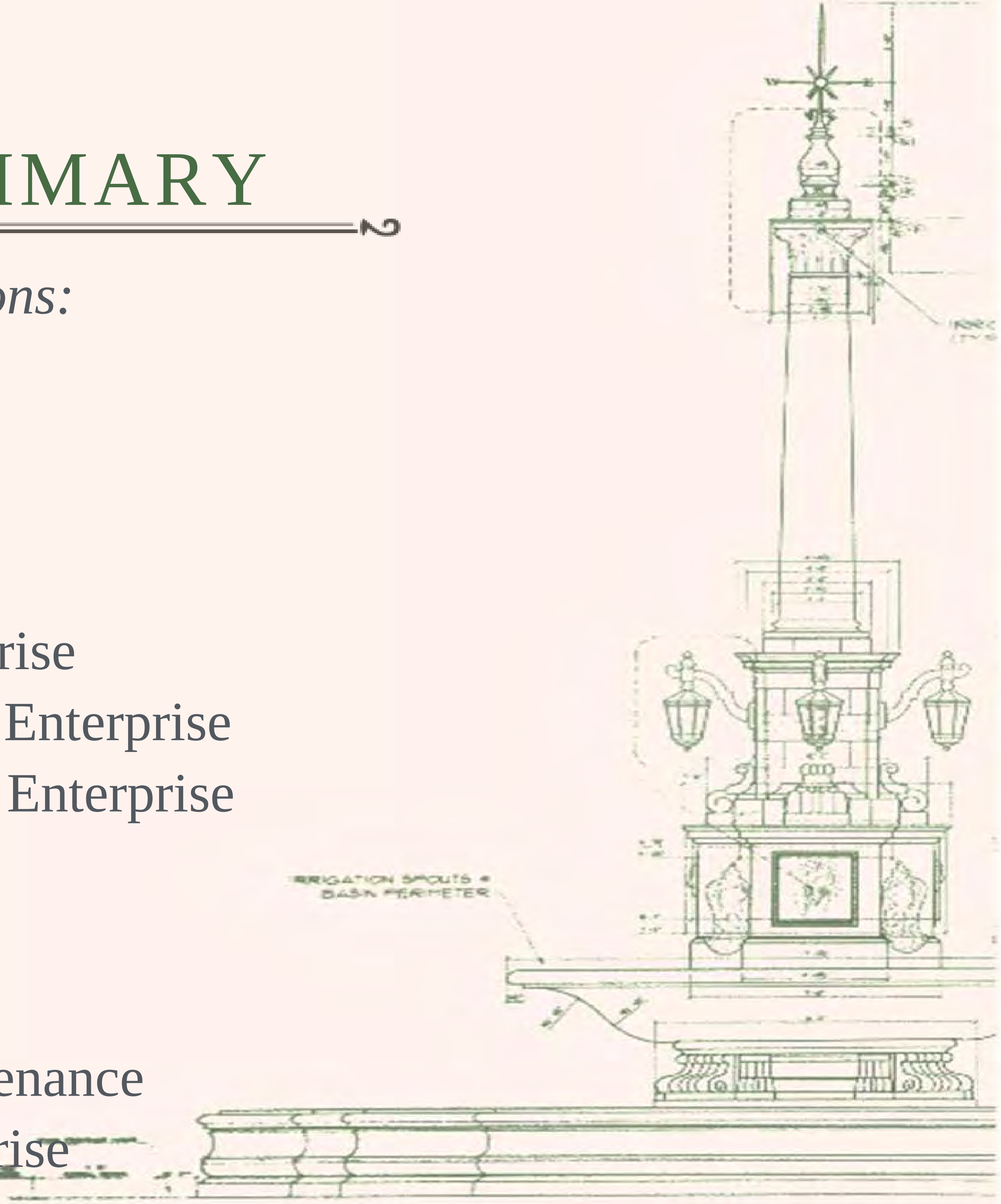
Community Recreation Facilities Include:

- Adult Activity Center
- Coral Gables Golf & Country Club:
  - Athletic Club
  - Country Club Venue
  - Granada Tennis Center
  - Granada Golf Course
  - Le Parc Café
- Girl Scout Little House - My Squad Lodge / DEI Clubhouse
- Salvadore Tennis Center
- Venetian Pool
- War Memorial Youth Center
- William H. Kerdyk Biltmore Tennis Center

EXECUTIVE SUMMARY

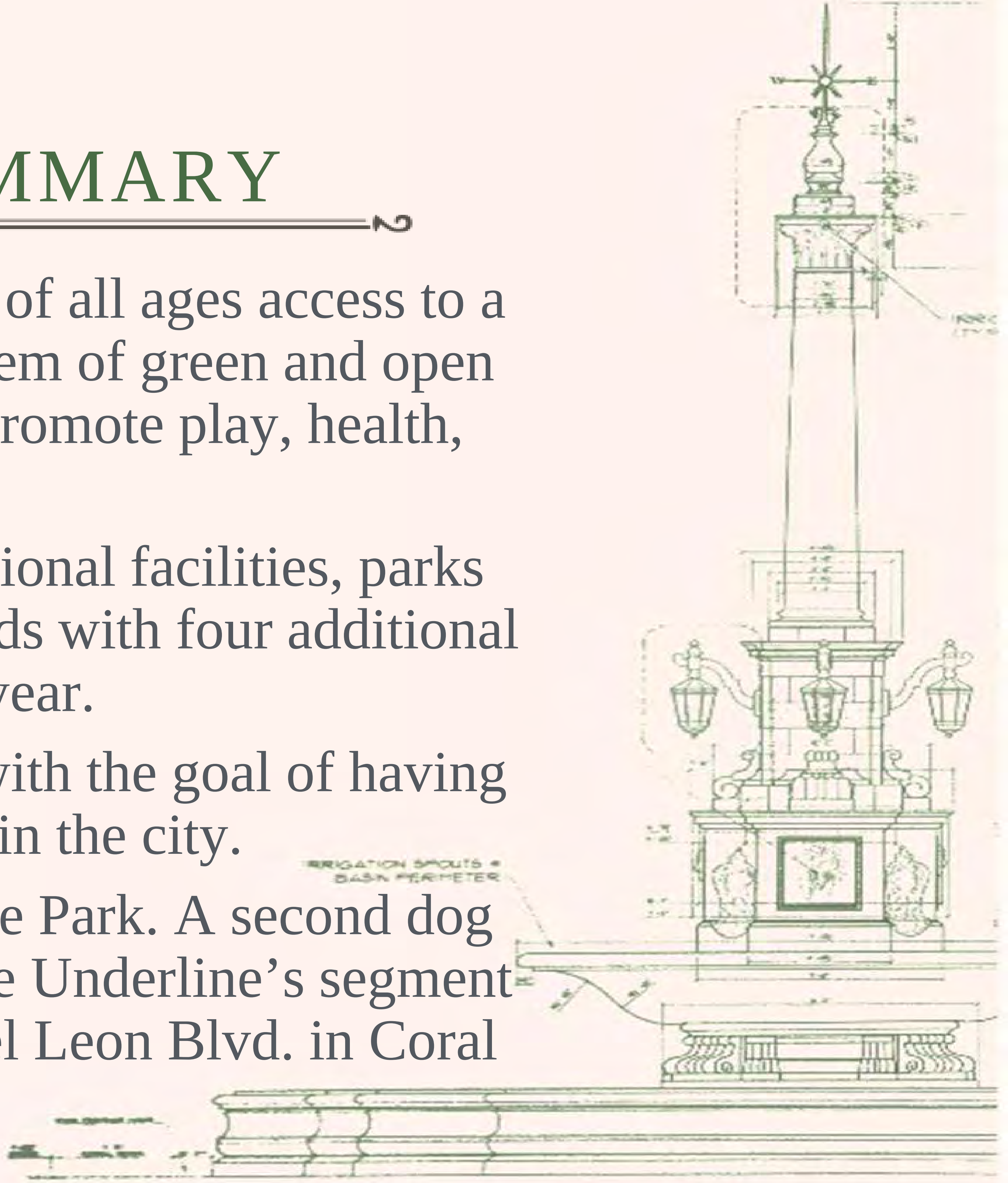
The Department now consists of 12 Divisions:

- 6000 – Administration
- 6010 – Tennis
- 6020 – Aquatics - Enterprise
- 6030 – Country Club Administration
- 6032 – Country Club Venue - Enterprise
- 6034 – Country Club Athletic Club - Enterprise
- 6038 – Country Club Granada Golf - Enterprise
- 6050 – Youth Center
- 6060 – Adult Services
- 6065 – Special Events
- 6070 – Golf Course and Parks Maintenance
- 6090 – Coral Gables Soccer - Enterprise



EXECUTIVE SUMMARY

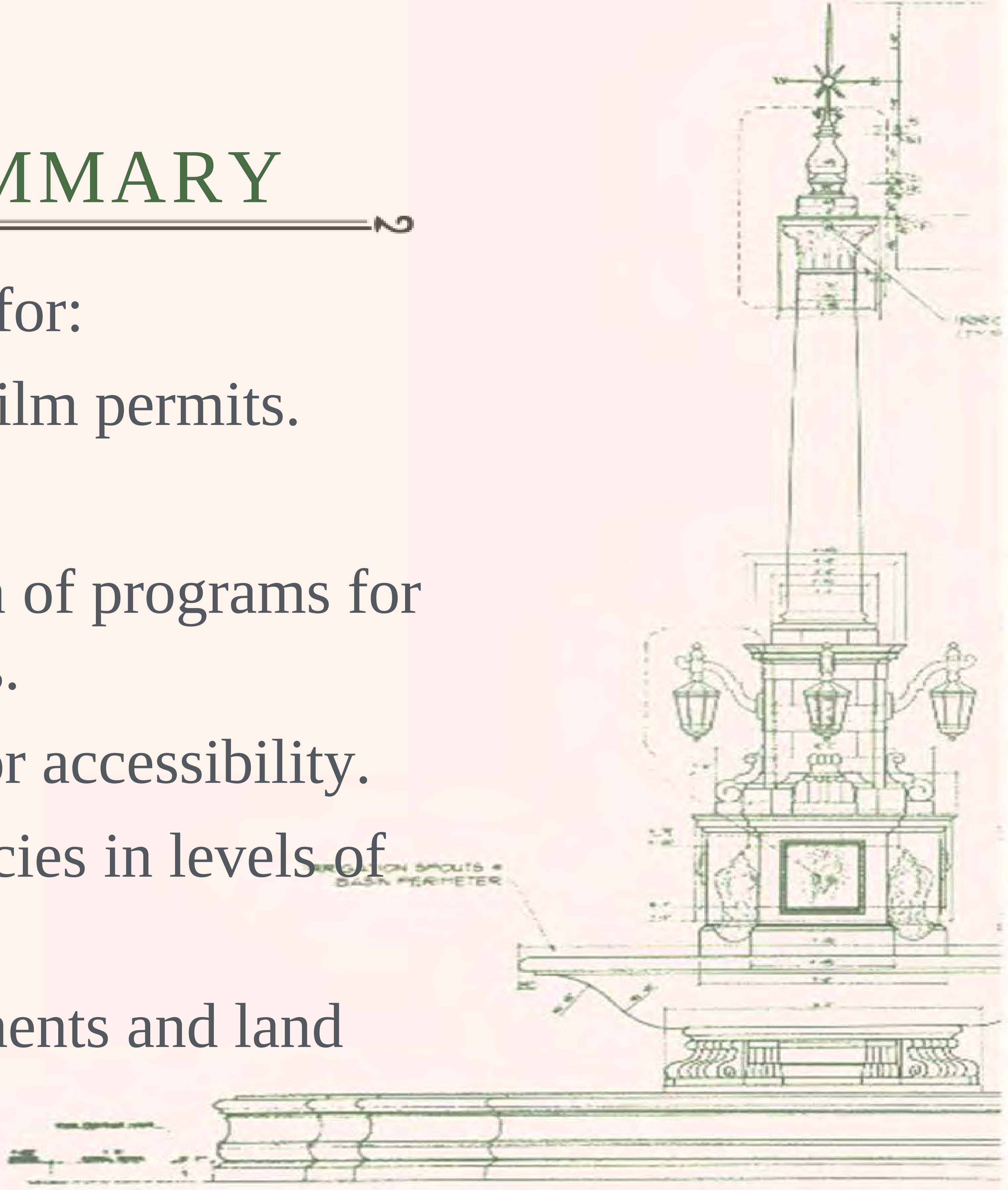
- City’s goal is to provide residents and guests of all ages access to a first-class and environmentally sensitive system of green and open spaces, facilities, programs, and events that promote play, health, and quality of life.
- Coral Gables has a combination of 68 recreational facilities, parks and open spaces which include 15 playgrounds with four additional playgrounds scheduled for construction this year.
- The city is committed to increase our parks with the goal of having a park within a 10-minute walk of any home in the city.
- The city opened its first dog park at Salvadore Park. A second dog park has been designed for construction at the Underline’s segment 5 at the corner of Le Jeune Rd. and Ponce Del Leon Blvd. in Coral Gables.



Executive Summary

The Department is also responsible for:

- Permitting of special events and film permits.
- Coordination of special events.
- Development and implementation of programs for cultural and recreational activities.
- Principles of inclusion to allow for accessibility.
- Identifying geographical deficiencies in levels of service for walkable parks.
- Coordination of capital improvements and land acquisitions.

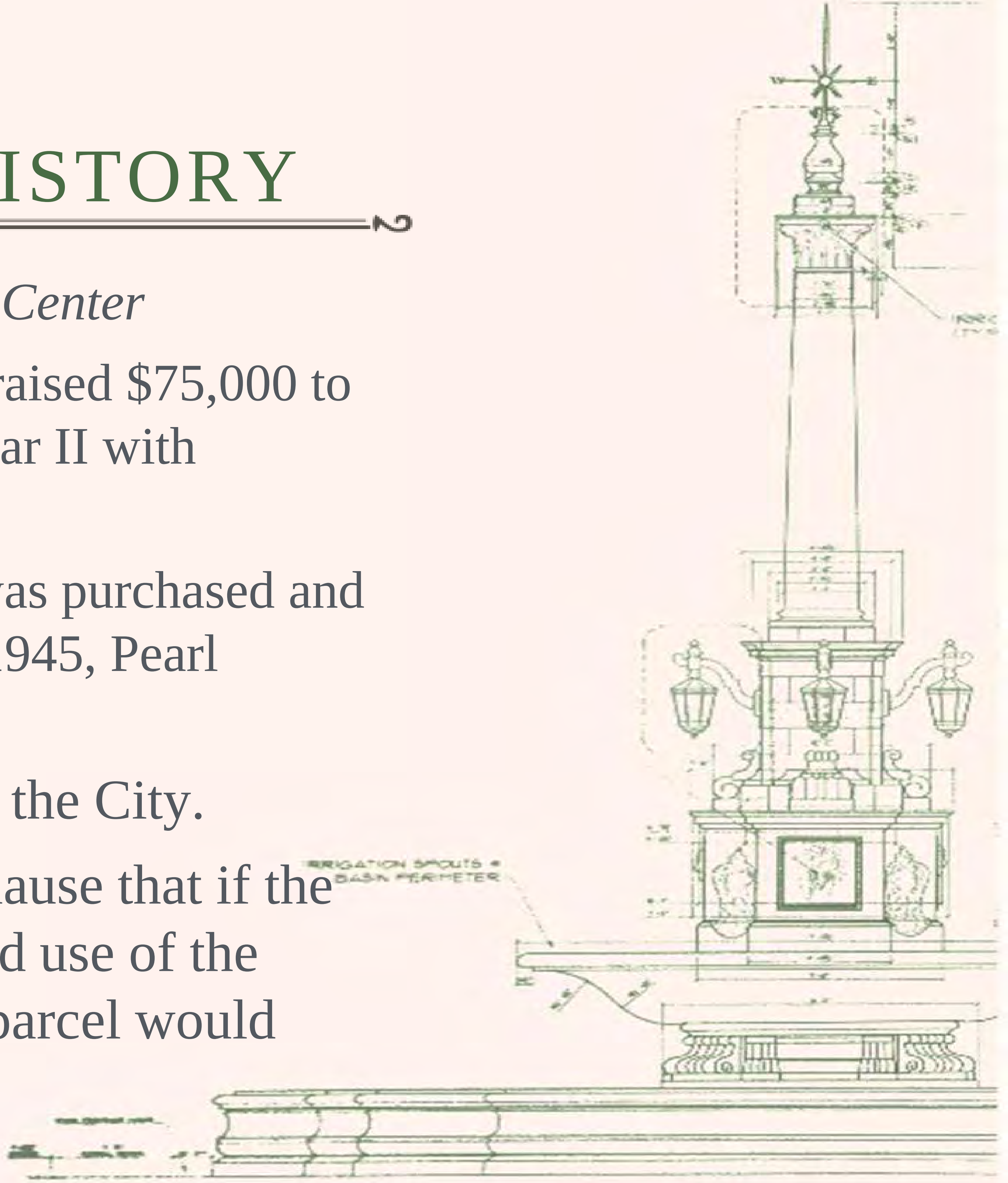


Business Identification

Department History

It all started with the War Memorial Youth Center

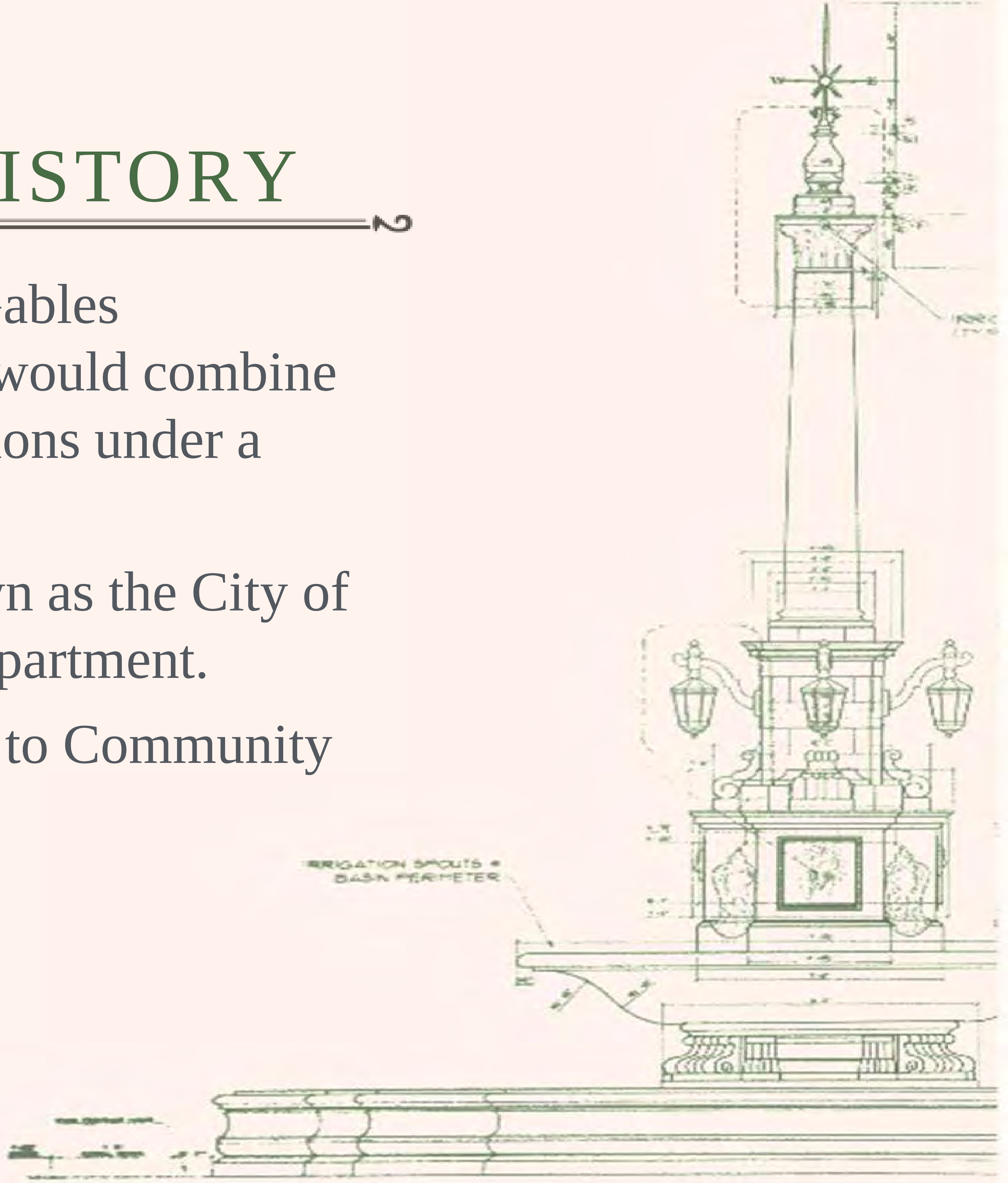
- In 1944 the War Memorial Association raised $75,000 to honor the youth who served in World War II with founding a youth recreation center.
- A site of 48 lots on Andalusia Avenue was purchased and the first center opened on December 7, 1945, Pearl Harbor Day.
- In 1956 the Center was turned over to the City.
- The Association included a reverter clause that if the City of Coral Gables ever discontinued use of the property as a youth center, the entire parcel would revert to the Association.



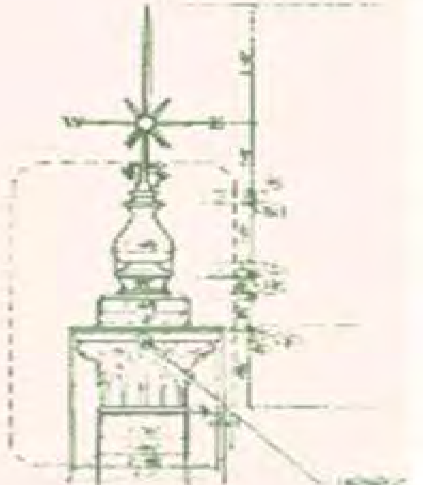
Department History

- In March of 1974, the City of Coral Gables implemented a new ordinance which would combine several different departments as divisions under a single department.
- The new department came to be known as the City of Coral Gables' Parks & Recreation Department.
- In 2018 the Department was renamed to Community Recreation Department.

COMMUNITY RECREATION



Mission, Vision, Values & Goals



MISSION:

Enhancing our community's quality of life through exceptional recreation opportunities.

VISION:

Creating community through memorable experiences.

Mission, Vision, Values & Goals

We **value** the quality of:

- **Le**adership and passion
- **I**ntegrity and accountability
- **F**amily and fun
- **E**nvironmentally and safety conscious

Focus Areas & Goals

- **Customer Focused Excellence:** Provide recreation opportunities innovatively, that elevate the customer experience while preserving our history.
- **Workforce Excellence:** Empower recreation professionals with the tools and guidance to provide excellent services.
- **Financial Excellence:** Utilize financial resources efficiently and ensuring sustainable cost recovery through responsible processes.
- **Process Excellence:** Ensure efficient and consistent business systems by optimizing best practices.
- **Community-focused Excellence:** Exceed community's expectations by striving to provide world-class facilities and services.
- **Sustainability-focused Excellence:** Protect and preserve the environment by identifying efficient, innovative and sustainable practices.

CITY OF CORAL GABLES

VINCE C. LAGO
MAYOR

RHONDA A. ANDERSON
VICE MAYOR

KIRK R. MENENDEZ
COMMISSIONER

MELISSA CASTRO
COMMISSIONER

ARIEL FERNANDEZ
COMMISSIONER

AMOS ROJAS Jr.
CITY MANAGER

CRISTINA M. SUAREZ, ESQ., B.C.S.
CITY ATTORNEY

BILLY Y. URQUIA
CITY CLERK

ALBERTO N. PARJUS
DEPUTY CITY MANAGER

JOE GÓMEZ, PE, TTCP, F. FES
ASSISTANT CITY MANAGER

DIANA M. GOMEZ, C.P.A
FINANCE DIRECTOR

PAULA A. RODRIGUEZ
ASSISTANT FINANCE DIRECTOR- MANAGEMENT, BUDGET & COMPLIANCE

PEDRO SANCHEZ
SR. MGMT & BUDGET ANALYST

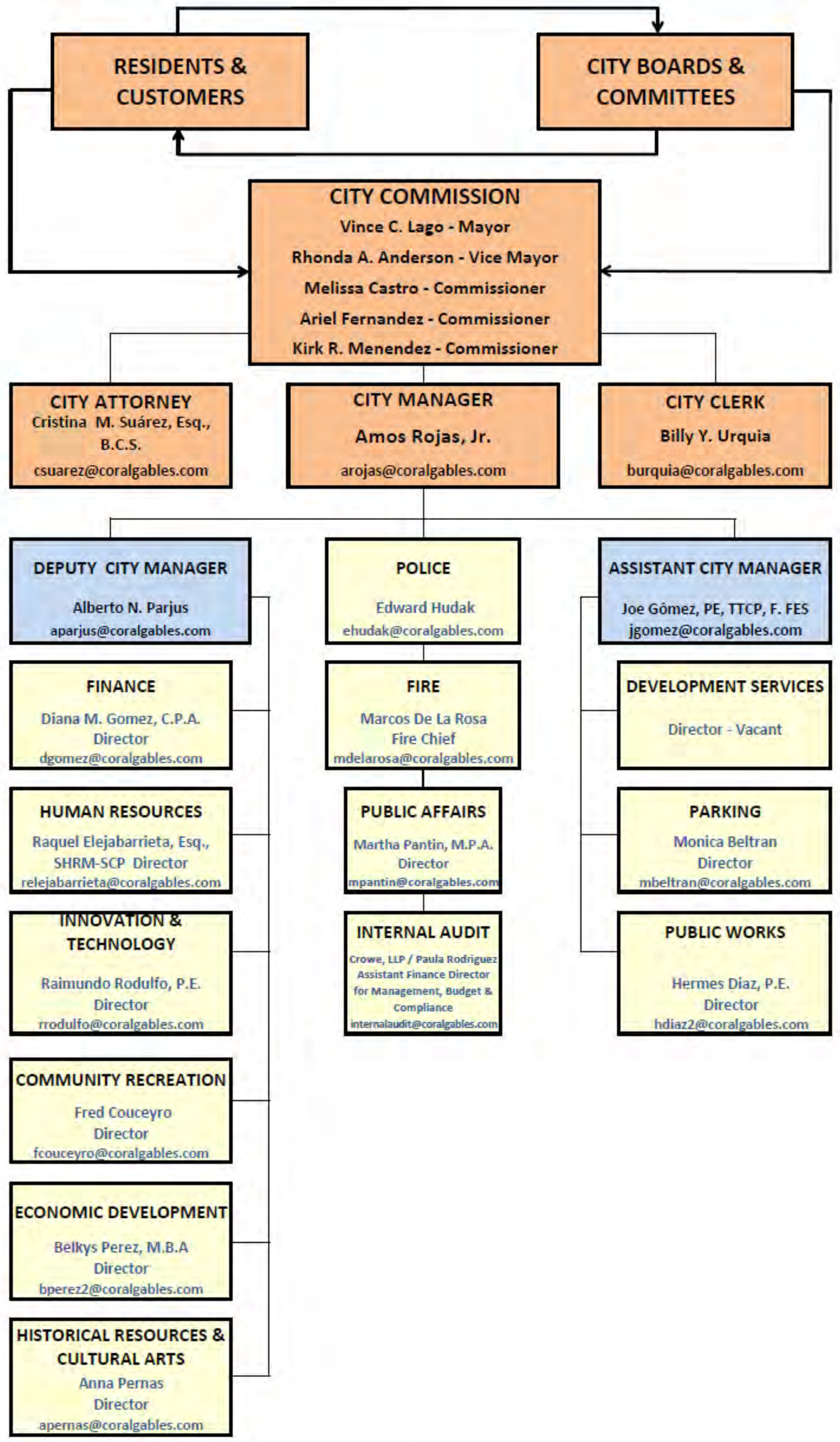
IVAN BAEZ
MGMT BUDGET ANALYST II

CHRISTOPHER GARCIA
MGMT BUDGET ANALYST II

ELSY FUENTES
INTERNAL AUDIT & GRANTS COORD.

ANAMY GARCIA
GRANTS COORDINATOR

CITY OF CORAL GABLES, FLORIDA
ORGANIZATION CHART
2024-2025 BUDGET



RESIDENTS & CUSTOMERS

CITY BOARDS & COMMITTEES

CITY COMMISSION
Vince C. Lago - Mayor
Rhonda A. Anderson - Vice Mayor
Melissa Castro - Commissioner
Ariel Fernandez - Commissioner
Kirk R. Menendez - Commissioner

CITY ATTORNEY
Cristina M. Suárez, Esq., B.C.S.
csuarez@coralgables.com

CITY MANAGER
Amos Rojas, Jr.
arojas@coralgables.com

CITY CLERK
Billy Y. Urquia
burquia@coralgables.com

DEPUTY CITY MANAGER
Alberto N. Parjus
aparjus@coralgables.com

POLICE
Edward Hudak
ehudak@coralgables.com

ASSISTANT CITY MANAGER
Joe Gómez, PE, TTCP, F. FES
jgomez@coralgables.com

FINANCE
Diana M. Gomez, C.P.A.
Director
dgomez@coralgables.com

FIRE
Marcos De La Rosa
Fire Chief
mdelarosa@coralgables.com

DEVELOPMENT SERVICES
Director - Vacant

HUMAN RESOURCES
Raquel Elejabarrieta, Esq., SHRM-SCP Director
relejabarrieta@coralgables.com

PUBLIC AFFAIRS
Martha Pantin, M.P.A.
Director
mpantin@coralgables.com

PARKING
Monica Beltran
Director
mbeltran@coralgables.com

INNOVATION & TECHNOLOGY
Raimundo Rodulfo, P.E.
Director
rrodulfo@coralgables.com

INTERNAL AUDIT
Crowe, LLP / Paula Rodriguez
Assistant Finance Director for Management, Budget & Compliance
internalaudit@coralgables.com

PUBLIC WORKS
Hermes Diaz, P.E.
Director
hdiaz2@coralgables.com

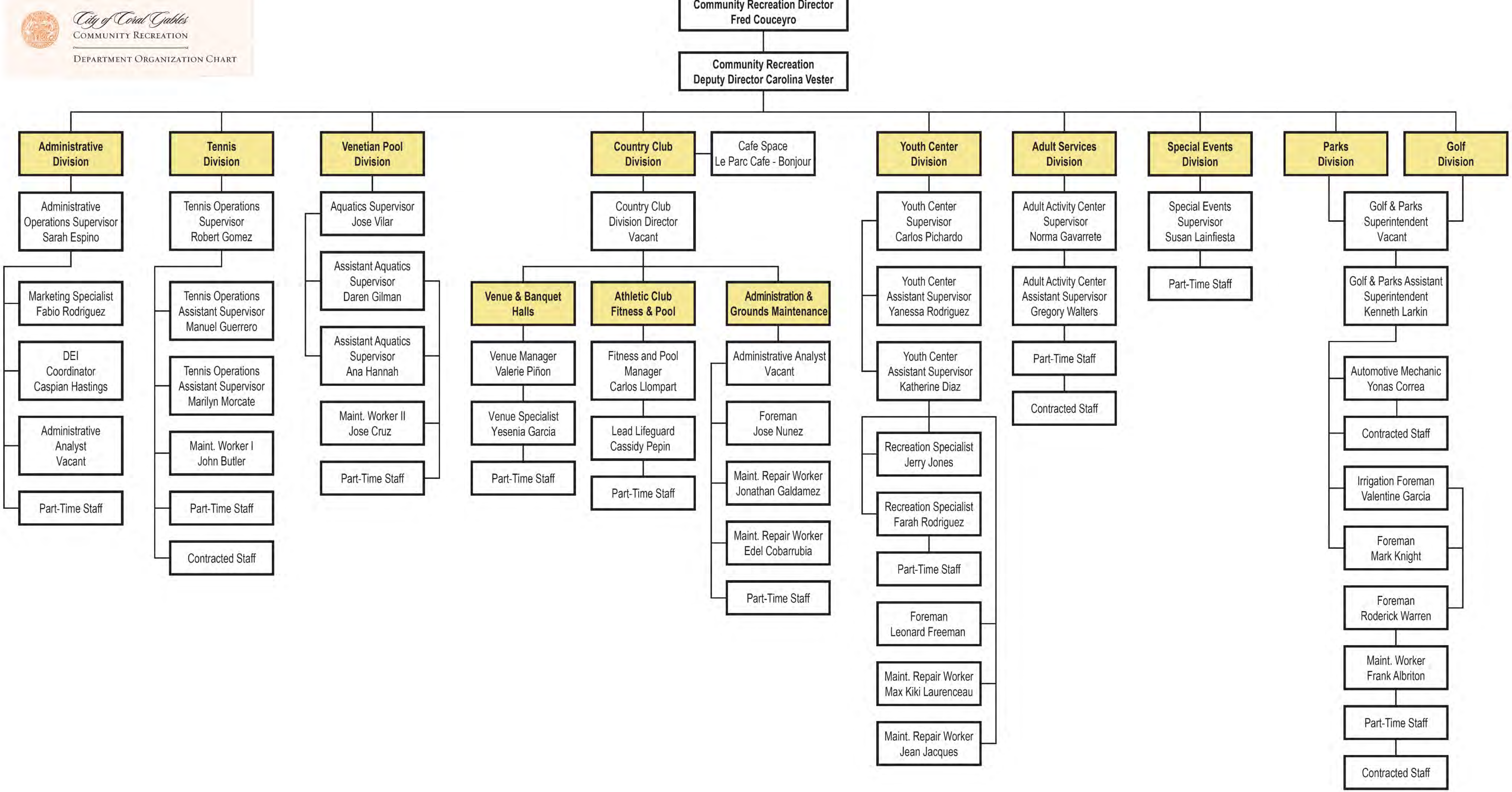
COMMUNITY RECREATION
Fred Couceyro
Director
fcouceyro@coralgables.com

ECONOMIC DEVELOPMENT
Belkys Perez, M.B.A
Director
bperez2@coralgables.com

HISTORICAL RESOURCES & CULTURAL ARTS
Anna Pernas
Director
apernas@coralgables.com

City of Coral Gables
Community Recreation

Department Organization Chart



Community Recreation Director
Fred Couceyro

Community Recreation
Deputy Director Carolina Vester

Administrative Division
- Administrative Operations Supervisor Sarah Espino
  - Marketing Specialist Fabio Rodriguez
  - DEI Coordinator Caspian Hastings
  - Administrative Analyst Vacant
  - Part-Time Staff

Tennis Division
- Tennis Operations Supervisor Robert Gomez
  - Tennis Operations Assistant Supervisor Manuel Guerrero
  - Tennis Operations Assistant Supervisor Marilyn Morcate
  - Maint. Worker I John Butler
  - Part-Time Staff
  - Contracted Staff

Venetian Pool Division
- Aquatics Supervisor Jose Vilar
  - Assistant Aquatics Supervisor Daren Gilman
  - Assistant Aquatics Supervisor Ana Hannah
  - Maint. Worker II Jose Cruz
  - Part-Time Staff

Country Club Division
- Cafe Space Le Parc Cafe - Bonjour
- Country Club Division Director Vacant
  - Venue & Banquet Halls
    - Venue Manager Valerie Piñon
    - Venue Specialist Yesenia Garcia
    - Part-Time Staff
  - Athletic Club Fitness & Pool
    - Fitness and Pool Manager Carlos Llompart
    - Lead Lifeguard Cassidy Pepin
    - Part-Time Staff
  - Administration & Grounds Maintenance
    - Administrative Analyst Vacant
    - Foreman Jose Nunez
    - Maint. Repair Worker Jonathan Galdamez
    - Maint. Repair Worker Edel Cobarrubia
    - Part-Time Staff

Youth Center Division
- Youth Center Supervisor Carlos Pichardo
  - Youth Center Assistant Supervisor Yanessa Rodriguez
  - Youth Center Assistant Supervisor Katherine Diaz
    - Recreation Specialist Jerry Jones
    - Recreation Specialist Farah Rodriguez
    - Part-Time Staff
    - Foreman Leonard Freeman
    - Maint. Repair Worker Max Kiki Laurenceau
    - Maint. Repair Worker Jean Jacques

Adult Services Division
- Adult Activity Center Supervisor Norma Gavarrete
  - Adult Activity Center Assistant Supervisor Gregory Walters
    - Part-Time Staff
    - Contracted Staff

Special Events Division
- Special Events Supervisor Susan Lainfiesta
  - Part-Time Staff

Parks Division
Golf Division
- Golf & Parks Superintendent Vacant
  - Golf & Parks Assistant Superintendent Kenneth Larkin
    - Automotive Mechanic Yonas Correa
    - Contracted Staff
    - Irrigation Foreman Valentine Garcia
    - Foreman Mark Knight
    - Foreman Roderick Warren
      - Maint. Worker Frank Albriton
      - Part-Time Staff
      - Contracted Staff

Trivia Question #1

HOW MANY DIVISIONS ARE THERE IN COMMUNITY RECREATION?

Correct Answer to Question #1

12 Divisions

Core Programs, Services & Facilities

PLAY for all

CORAL GABLES ACCESSIBLE RECREATION

Stewards

CAPRA Accredited

Adventure Day

Diversity Equity Inclusion

Marketing

Special Projects

Transition Support

Capital Improvements

Internships

Land Acquisition

My Squad

RecTrac

Administration – Division 6000

Doubles Drills

Social Play

League Play

High Performance Instruction

Ladies Teams

Private Lessons

Varsity Clinics

Junior Varsity Clinics

Adult Beginners Clinics

Camps

Tournaments

My First Tennis Camps

Tennis– Division 6010

CORAL GABLES
THE CITY BEAUTIFUL

Romance Under the Stars

Jr Lifeguard Camp

Paws in the Pool

Public Swim Entry

Lifeguard Classes

Guard Start

Pumpkin Float

Fun in the Sun Camp

Swim Lessons

Historic Landmark

Water Safety Instructor Classes

Pool Membership

Aquatics Venetian Pool– Division 6020

CORAL GABLES
THE CITY BEAUTIFUL

Athletic Club

Kids Club

Junior Olympic Sized Pool

Exercise Classes

Public Greens Fees

Special Events

Le Parc Cafe

Golf Tournaments

Membership

Neighborhood Tennis

Venue Rentals

Community Events

Teen Program

Haunted House

Gymnastics

Youth Sports

Fitness Membership & Classes

Leagues

Bricks for Kidz STEM

Special Events

Theater Productions

Camps

Club Play Aftercare

Dance

Youth Center– Division 6050

Salsa

Wii Fit

Yoga

Aqua Zumba

Pilates

Ballet

Life In Motion

Tai Chi

Stretch

Total Body

Zumba

Pickle Ball

Farmers Market

Memorial Day Celebration

Hot Chocolate with Santa

Pumpkin Patch

Permits

Holiday Park

Holiday Tree Lighting

Literacy Festival

Eggstreme Egg Hunt

Big Toy

4th of July

Movies under the Gables Moonlight

Special Events & Permits– Division 6065

5 Minute

Break

CORAL GABLES
THE CITY BEAUTIFUL

Trivia Question #2

WHAT IS THE CITY'S VISION STATEMENT?

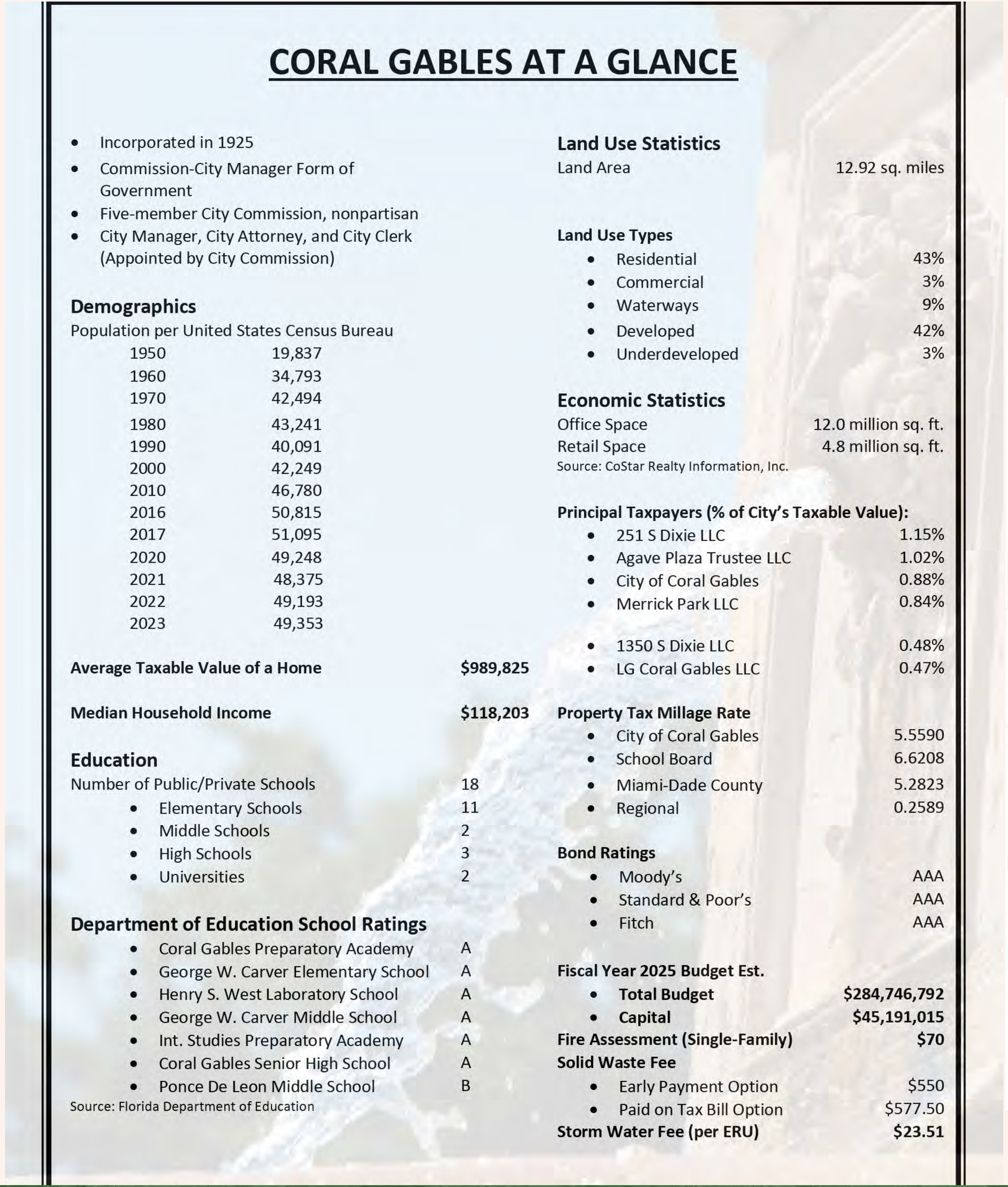
Correct Answer to Question #2

“A world-class City
with a Hometown Feel”

Marketing Analysis

Market Segregation

- Coral Gables serves a population of approximately 49,353 based on the 2023 estimate.
- The Department served over 22,000 registered participants this past year. *This does not include one-time transactional customers and visitors.*



CORAL GABLES AT A GLANCE

- Incorporated in 1925
- Commission-City Manager Form of Government
- Five-member City Commission, nonpartisan
- City Manager, City Attorney, and City Clerk (Appointed by City Commission)

Demographics

Population per United States Census Bureau

1950	19,837
1960	34,793
1970	42,494
1980	43,241
1990	40,091
2000	42,249
2010	46,780
2016	50,815
2017	51,095
2020	49,248
2021	48,375
2022	49,193
2023	49,353

Average Taxable Value of a Home	**$989,825**
Median Household Income	**$118,203**

Education

Number of Public/Private Schools	18
• Elementary Schools	11
• Middle Schools	2
• High Schools	3
• Universities	2

Department of Education School Ratings

• Coral Gables Preparatory Academy	A
• George W. Carver Elementary School	A
• Henry S. West Laboratory School	A
• George W. Carver Middle School	A
• Int. Studies Preparatory Academy	A
• Coral Gables Senior High School	A
• Ponce De Leon Middle School	B

Source: Florida Department of Education

Land Use Statistics

Land Area	12.92 sq. miles

Land Use Types

• Residential	43%
• Commercial	3%
• Waterways	9%
• Developed	42%
• Underdeveloped	3%

Economic Statistics

Office Space	12.0 million sq. ft.
Retail Space	4.8 million sq. ft.

Source: CoStar Realty Information, Inc.

Principal Taxpayers (% of City's Taxable Value):

• 251 S Dixie LLC	1.15%
• Agave Plaza Trustee LLC	1.02%
• City of Coral Gables	0.88%
• Merrick Park LLC	0.84%
• 1350 S Dixie LLC	0.48%
• LG Coral Gables LLC	0.47%

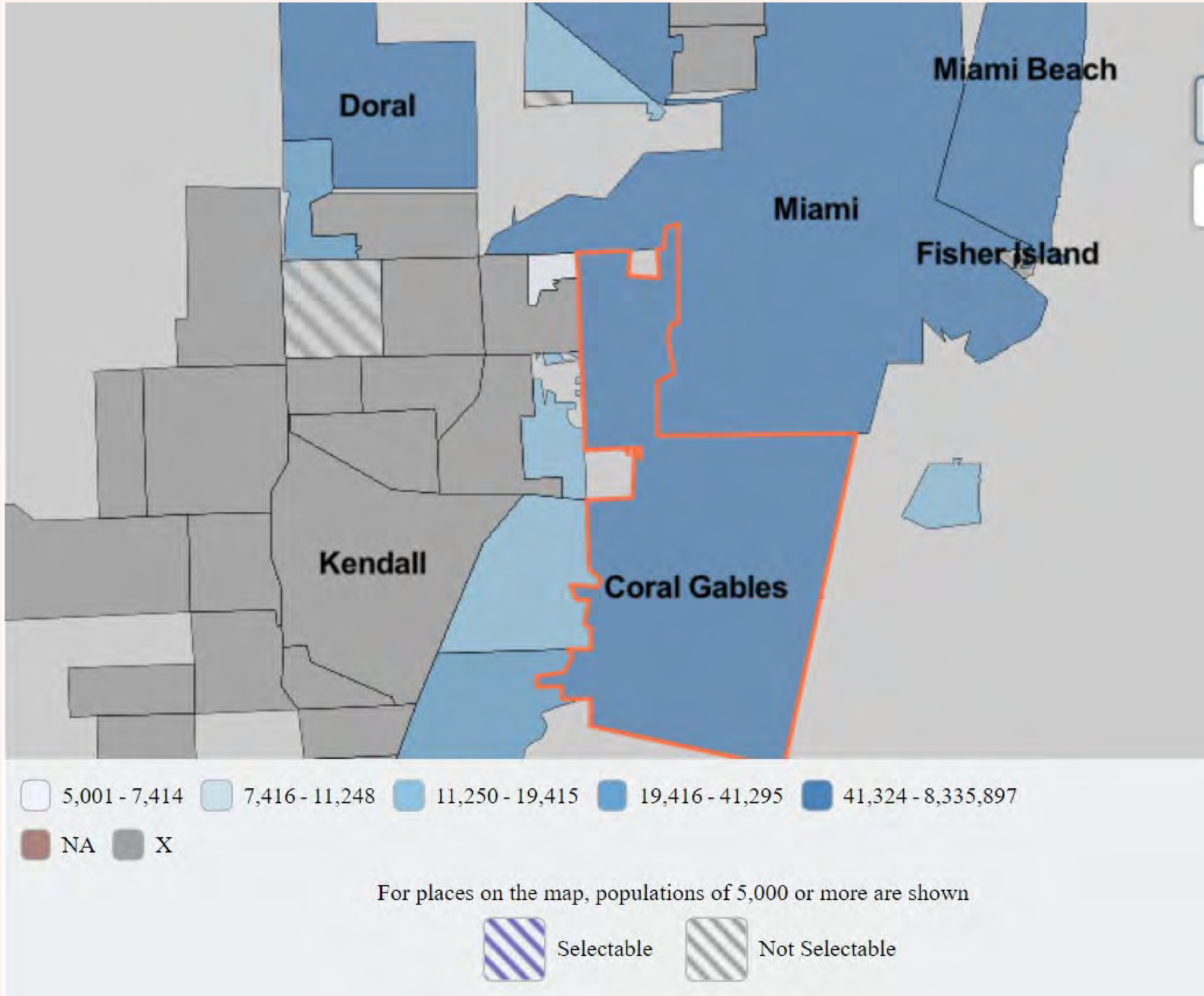
Property Tax Millage Rate

• City of Coral Gables	5.5590
• School Board	6.6208
• Miami-Dade County	5.2823
• Regional	0.2589

Bond Ratings

• Moody's	AAA
• Standard & Poor's	AAA
• Fitch	AAA

Fiscal Year 2025 Budget Est.	
• **Total Budget**	**$284,746,792**
• **Capital**	**$45,191,015**
Fire Assessment (Single-Family)	**$70**
Solid Waste Fee	
• Early Payment Option	$550
• Paid on Tax Bill Option	$577.50
Storm Water Fee (per ERU)	**$23.51**



Service Area

- The City of Coral Gables Community Recreation Department provides priority access to City of Coral Gables residents through early registration opportunities and reduced resident fees.
- Approximately 48.34% of its registered customer base are Coral Gables Residents.
- Approximately 51.66% are non-residents, and include Miami-Dade County residents and other national and international visitors.

THE CITY OF CORAL GABLES IS LOCATED IN MIAMI DADE COUNTY AND IS A VERTICAL CITY THAT RUNS FROM NORTH TO SOUTH. THE CITY BORDERS THE CITY OF WEST MIAMI, CITY OF SOUTH MIAMI, CITY OF PINECREST AND CITY OF COCONUT GROVE.

THE CITY IS HORIZONTALLY DISSECTED BY MAJOR ARTERIAL ROADS SUCH AS TAMIAMI TRAIL, CORAL WAY, BIRD ROAD, US1, AND SUNSET DRIVE.

TWO POTENTIAL ANNEXATIONS INCLUDE LITTLE GABLES IN THE NORTH AND HIGH PINES IN THE SOUTH.

POINTS OF INTEREST

** Locally designated historic sites*
*** Nationally & locally designated historic sites*
**** Florida Historical Marker*

GOVERNMENT & COMMUNICATIONS

MUNICIPAL:

1	Coral Gables City Hall **	E-4
2	Coral Gables Police and Fire Station	E-4
3	Fire Station #2	D-7
4	Doris & Phil Sanford Fire Station #3	B-15
41	Coral Gables Museum **	E-3

COUNTY:

5	Miami-Dade County District Court	E-4
6	Coral Gables Public Library	D-5
7	Metrorail Station (University)	C-8
8	Metrorail Station (Douglas Road)	E-6
10	Passport Acceptance Facility	E-6

FEDERAL:

12	U.S. Post Office (two locations)	E-4, F-4

HISTORIC SITES, FOUNTAINS, PLAZAS AND ENTRANCES

152	Alcazar Avenue Historic District	D-3 – E-3
153	Alhambra Circle Historic District	B-4 – E-3
14	Alhambra Entrance *	F-3
15	Alhambra Plaza *	F-3
16	Alhambra Water Tower *	C-3
17	Balboa Plaza *	D-4
18	Biltmore Hotel and Country Club **	C-5
134	Campina Court Historic District *	F-1
19	Cartagena Plaza	E-10
100	George Washington Carver School *	E-7
154	Castille Ave/Plaza Historic District	B-3 – C-3
20	Chinese Village *	D-7
50	Church of the Little Flower Historic District *	B-4
21	Cocoplum Woman's Club *	B-10
1	Coral Gables City Hall Historic District *	E-4
24	Coral Gables Congregational Church **	C-4
101	Coral Gables Preparatory Academy **	E-3
25	Coral Gables Merrick House **	C-3
137	Coral Gables Waterway ***	D-6 – F-10
26	Coral Gables Woman's Club **	E-2
27	Coral Way Entrance	B-3
156	Coral Way Historic District	C-3
28	Country Club of Coral Gables *	C-3
29	Country Club of Coral Gables Historic District *	B-3, D-3
30	Country Club Prado Entrance *	B-2
31	Doc Dammers' House *	C-3
32	De Soto Fountain *	C-4
33	Douglas Entrance **	F-2
34	Dutch South African Village *	E-9
157	H. George Fink Studio	E-4
23	Florida Pioneer Village *	C-6
35	French City Village *	C-8
36	French Country Village *	D-8
37	French Normandy Village *	E-5
38	Granada Entrance *	C-2
77	Granada Golf Course *	D-3
39	Granada Plaza *	C-3
40	Italian Village *	D-6
127	MacFarlane Homestead Historic District **	E-6
82	Matheson Hammock County Park and Marin *	C-13
11	Miracle Mile Gate	F-4
67	Miracle Theatre *	E-4
138	Old Cutler Road ***	E-10 – B-15
41	Old Police and Fire Station/ Coral Gables Museum **	E-3
151	Obispo Avenue Historic District	B-3 – D-3
42	Pinewood Cemetery *	D-10
105	Ponce de Leon Middle School *	C-8
43	Rotunda at the Colonnade Hotel *	E-3
150	Santa Maria Street Historic District	C-6
135	Santiago Street Historic District *	D-2
44	Venetian Pool **	C-4
47	White Way Lights	D-5
136	Women Take Action in Coral Gables *** (The Roxcy O'Neal Bolton House)	B-3

HOSPITALS

45	Coral Gables Hospital	E-4
46	Doctors' Hospital	C-7

HOUSES OF WORSHIP

48	Cathedral of St. George	E-4
49	Central Christian Church of Dade County	E-2
50	Church of the Little Flower *	B-4
51	Coral Gables Baptist Church	D-8
24	Coral Gables Congregational Church **	C-4
52	Episcopal Church Center, U of M/Chapel of the Venerable Bede	C-8
53	First Church of Christ, Scientist, of Coral Gables and Reading Room	E-4
55	First United Methodist Church of Coral Gables	D-4
56	First United Methodist Church of South Miami	B-9
58	Granada Presbyterian Church	C-5
59	Hillel Jewish Student Center, U of M	C-8
60	Miami Friends (Quaker)	C-10
61	Riviera Presbyterian Church	C-10
62	St. Augustine Catholic Church	B-8
63	St. James Evangelical Lutheran Church	E-2
64	St. Mark's Lutheran Church of Coral Gables	E-5
126	St. Mary's First Missionary Baptist Church	E-6
65	St. Philip's Episcopal Church	C-4
128	St. Thomas Episcopal Church	B-11
66	Temple Judea	D-8
68	University Baptist Church	D-5
69	Wesley United Methodist	F-1

PARKS AND RECREATION

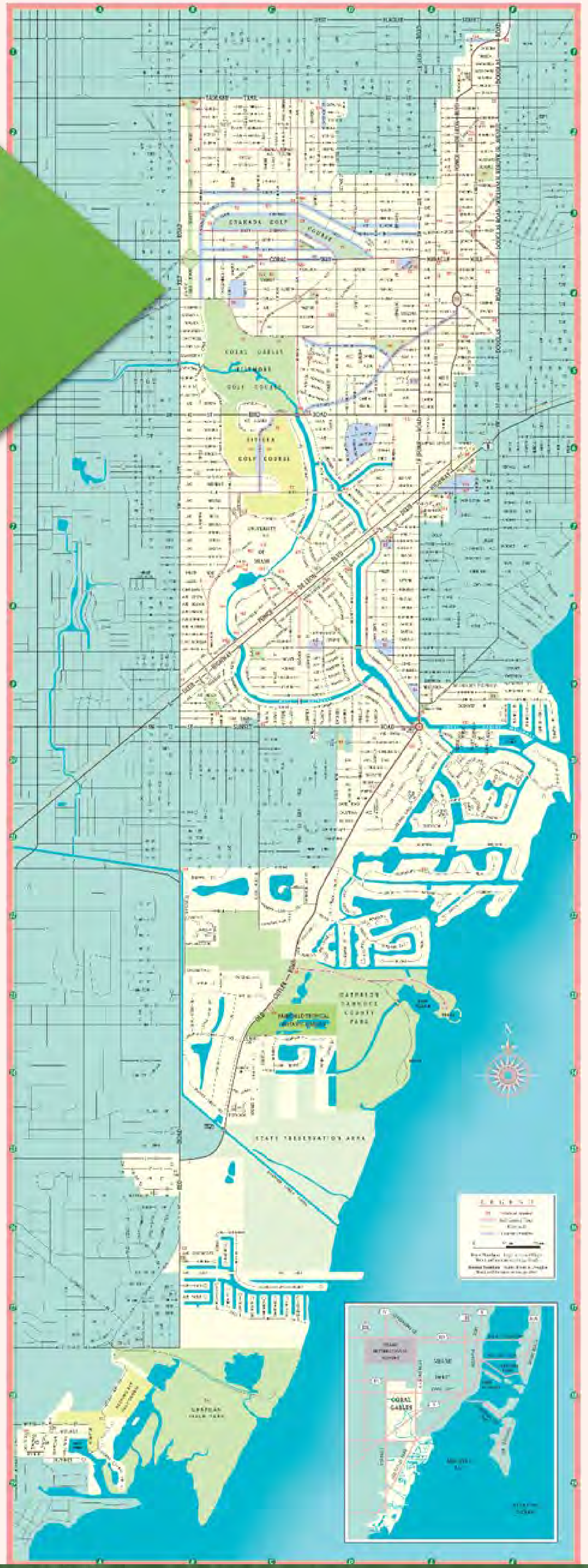
159	Adult Activity Center	F-4
70	Alcazar Plaza	D-3
155	Betsy Adams and Coral Gables Garden Club Park	B-6
71	City of Coral Gables Biltmore Golf Course (public)	B-4
97	William A. Cooper Park	E-7
72	William H. Kerdyk Biltmore Tennis Center	C-5
91	William H. Kerdyk, Jr. and Family Park	B-9
161	Blue Road Open Space	D-7
9	Butterfly Garden	D-5
120	Catalonia Park	D-4
165	Enrique "Henry" Cepero Memorial Park	B-6
54	Chapman Field Park	A-18
73	Coral Bay Park	B-16
74	Coral Gables War Memorial Youth Center	E-5
167	Country Club Prado	B-2
57	Deering Bay Country Club (private)	A-18
164	Durango Park	C-5
75	Fairchild Tropical Botanic Garden	C-13
129	Robert J. Fewell Park	C-4
130	Freedom Plaza	F-2
76	J. Fritz and Frances Gordon Park	B-2
77	Granada Golf Course * (public)	D-3
78	Granada Park	C-7
88	Fred B. Hartnett Ponce Circle Park	E-4
79	Ingraham Park	E-9
80	Jaycee Park	C-9
139	Carlos S. Kakouris Park	C-7
166	Leucadendra Drive Triangle	E-11
162	Lisbon Park	B-2
81	MacFarlane Linear Park	E-6
140	Maggiore Park	D-7
164	Mall Street Median	D-8
159	Marlin Park	A-19
82	Matheson Hammock County Park and Marina *	C-13
83	Merrick Park	E-4
163	Majorca Park	C-3
84	Nellie B. Moore Park	E-7
133	Orduna Drive/Miller Road Triangle	D-8
141	Ruth Bryan Owen Waterway Park	C-6
132	Perrin Plaza	E-3
85	Phillips Park	F-2
86	Pierce Park	E-6
87	Pittman Park	E-3
89	Ponce de Leon Park	E-2
90	Riviera Country Club (private)	C-6
144	Alex Rodriguez Park	C-8
22	Rotary Centennial Park	E-1
166	Salvadore Park	C-4
92	Salvadore Tennis Center	C-4
131	San Sebastian Park	E-4
169	Sarto Green Space	E-5
93	Loretta Sheehy Park	E-9
94	Sunrise Harbor Park	F-9
170	Tiziano Park	D-10
95	University Park	D-5
13	Venetia Park	C-2
44	Venetian Pool **	C-4
96	Lola B. Walker Pioneers' Park	E-7
98	Nat Winokur Park	E-6
99	Young Park	C-3

SCHOOLS

100	George W. Carver School *	E-7
101	Coral Gables Preparatory Academy **	E-3
102	Coral Gables Senior High School	E-6
103	Gulliver Academy	B-16
104	Merrick Educational Center	F-3
105	Ponce de Leon Middle School *	C-8
106	Riviera Day School	B-9
65	Saint Philip's Episcopal School	C-4
50	Saint Theresa School	B-4
128	St. Thomas Episcopal School	B-11
107	Henry S. West Lab School	C-7

UNIVERSITY OF MIAMI

110	Ashe Administration Building	C-7
148	Cosford Cinema	C-7
114	Gusman Concert Hall	C-7
145	Herbert Wellness Center	C-8
143	Herman Ring Theatre	C-7
116	Shalala Student Center	C-7
160	The Lennar Foundation Medical Center	B-8
121	Lowe Art Museum and Palley Pavilion	C-8
147	Pavia and Merrick Garages	C-8
112	Richter Library	C-7
146	Ponce de Leon Garage and UM Police	C-8
142	Watsco Center	C-8
122	Whitten University Center	C-7

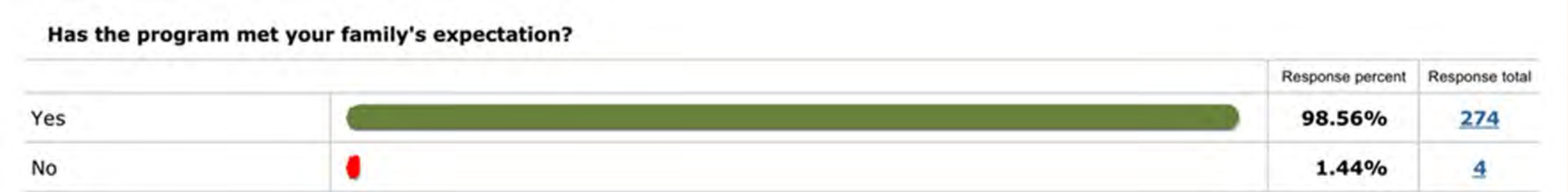


Competition

- Geographically, the City of Coral Gables predominantly competes for land and space with Miami Dade County parks and neighboring parks in cities such as:
  - West Miami
  - South Miami
  - Pinecrest
  - Coconut Grove
- Property values in the City are extremely high and new parcels of land are difficult to acquire.
- Due to lack of space, we compete with the County’s large playgrounds, natural parks & trails, waterparks, dog parks and etc.

Competition

- The transactional key requirements survey identified that the four most important aspects for participants in selecting to participate in City programs and activities are:
  - Location
  - Safe Facilities
  - Instructor to Student Ratio
  - Friendly Staff
- As part of the survey, 98.56% of participants felt that the City programs met their family's expectations.

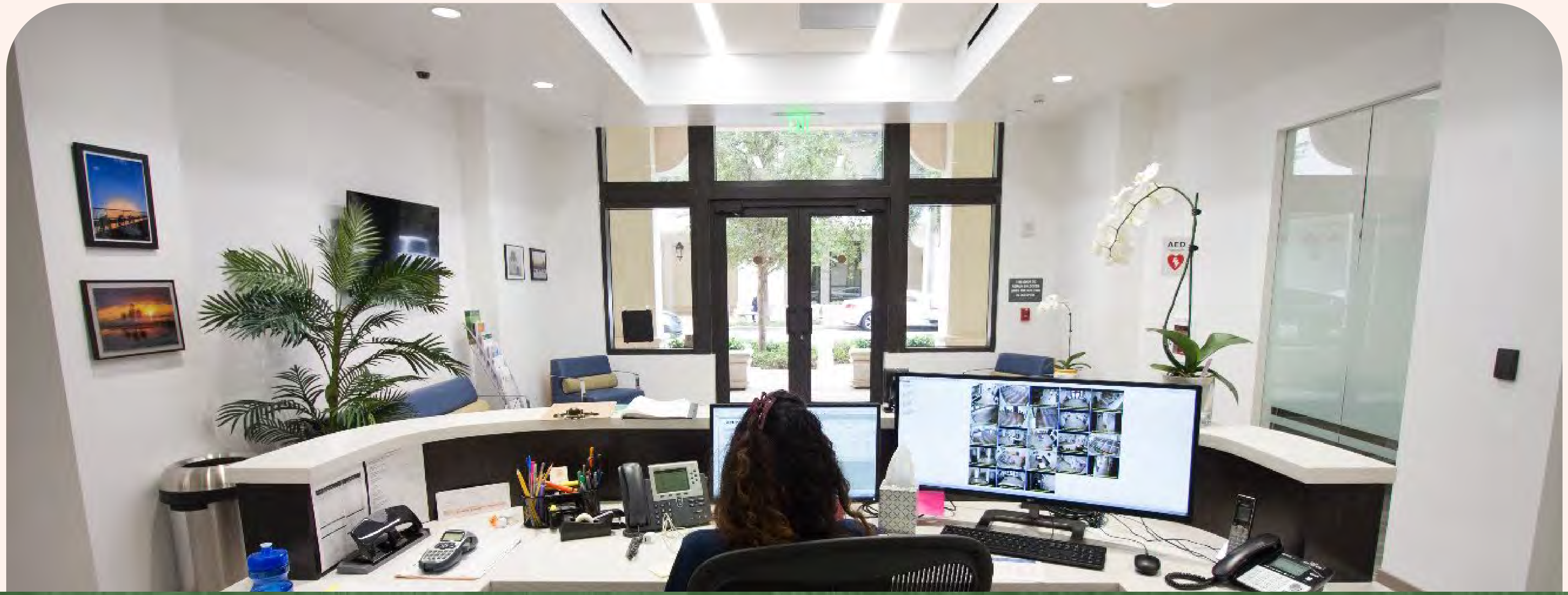


Has the program met your family's expectation?

		Response percent	Response total
Yes		98.56%	274
No		1.44%	4

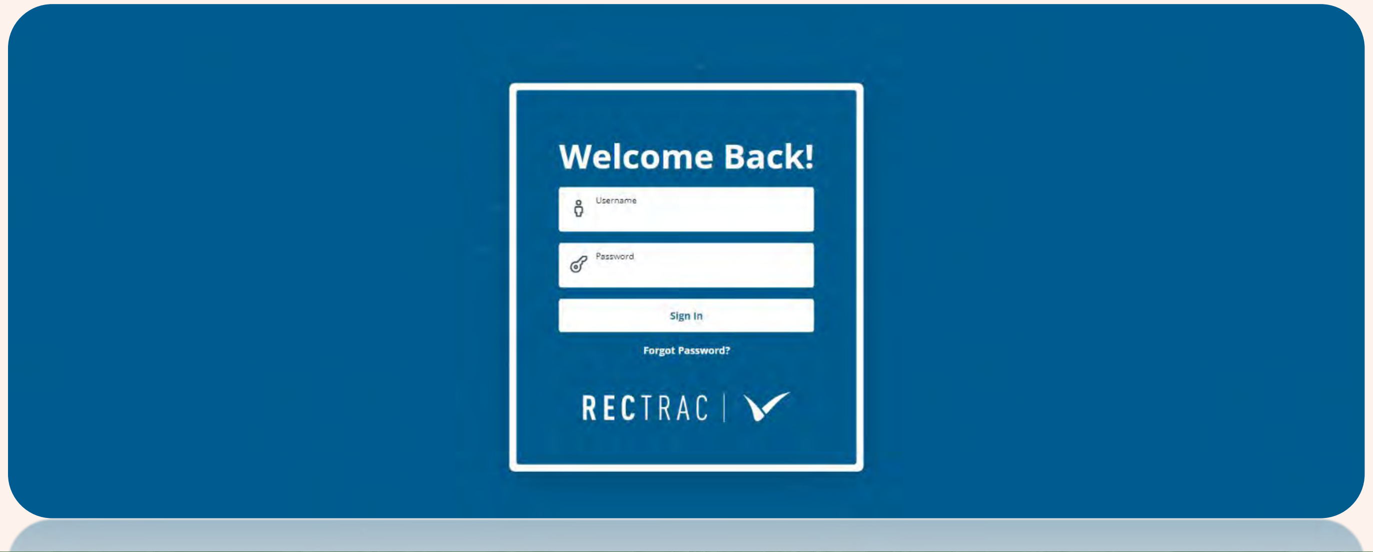
Trends

- The Community Recreation Department annually reviews the needs of the community and tasks each Division to identify a local, national and international trend in their industry to ensure that programming stays relevant.
- In addition, an evaluation is conducted by staff following each program to review participant attendance and satisfaction.



TRENDS

- The largest industry trend continues to be that of technology, and the customer demand for making the registration process accessible on the go and as simple as possible.
- In 2018 the Community Recreation Department migrated from a legacy recreation software to a hosted recreation software that allows participants to register and pay for services remotely.



Welcome Back!

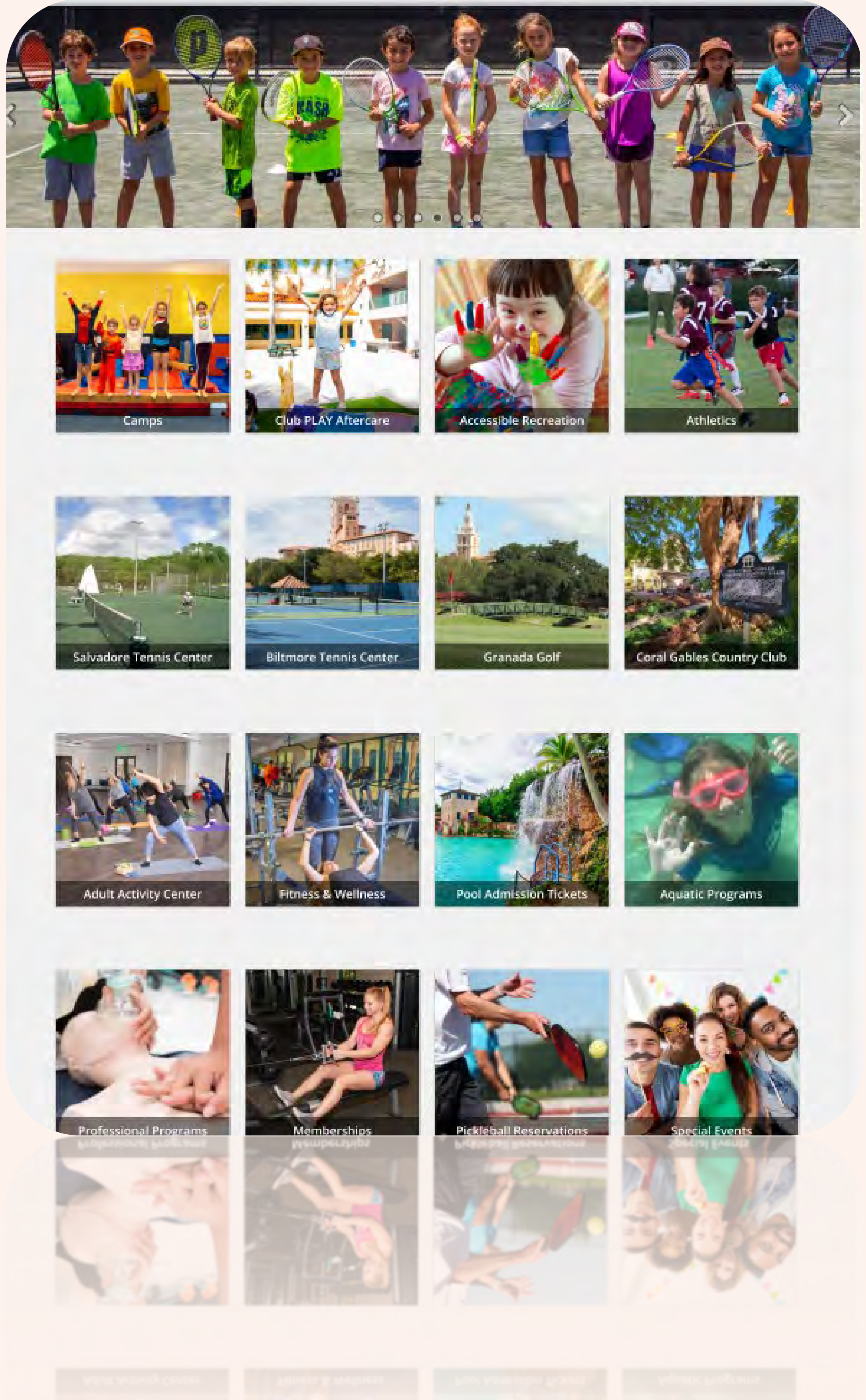
Username

Password

Sign In

Forgot Password?

RECTRAC |



Trivia Question #3

WHAT IS THE FULL NAME OF THE FOUNDER OF CORAL GABLES?

Correct Answer to Question #3

GEORGE EDGAR MERRICK

Operations Analysis

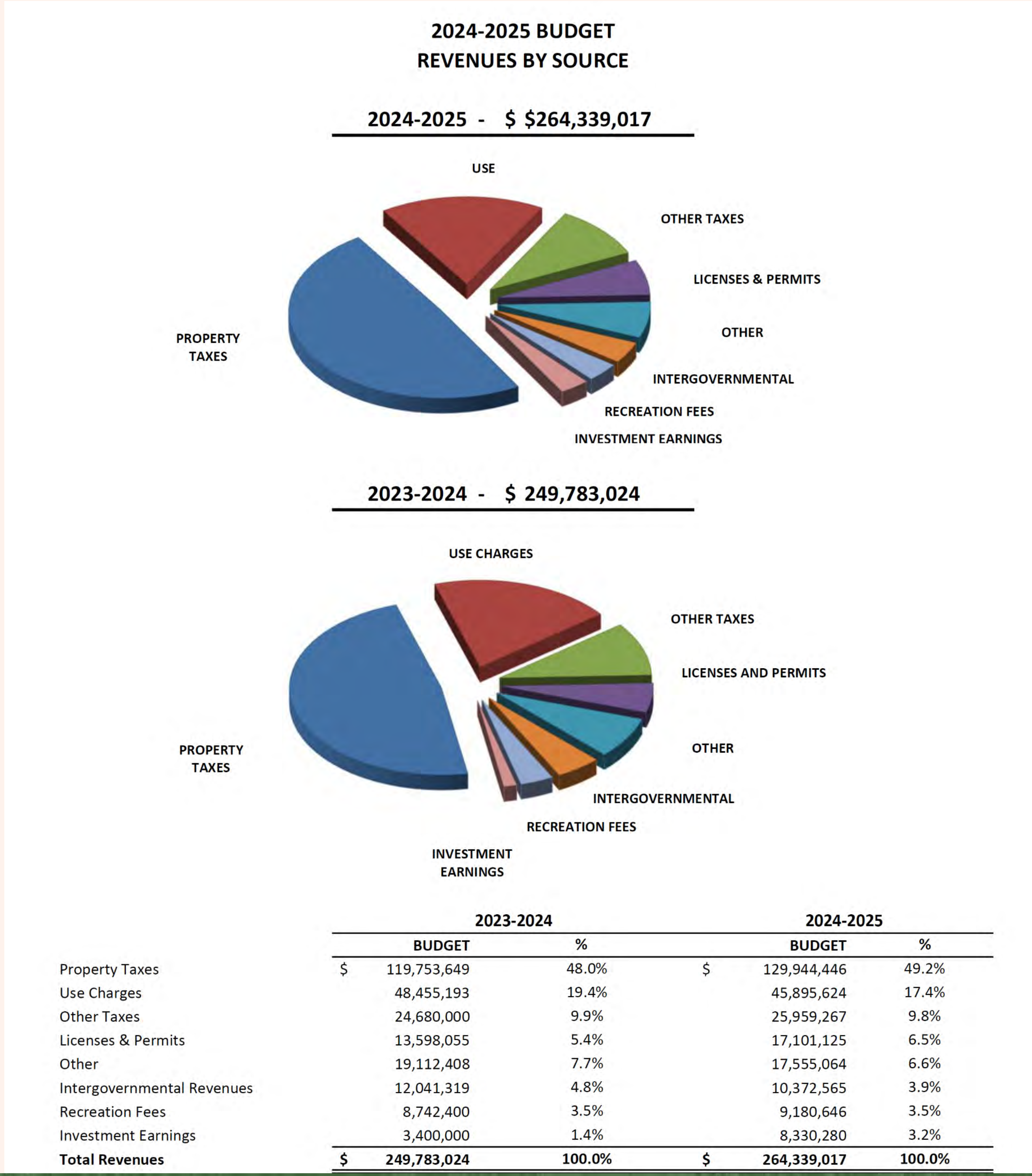
Summary of Expenses and Revenues

- The Community Recreation budget differs from other City Department budgets because many of the expenditure accounts are revenue driven.
- Venetian Pool and Coral Gables Golf and Country club are examples of an Enterprise Fund.
- Enterprise Funds - are self funded/sustainable and may drive a small profit.
- Cost recovery is an important aspect within the Department
- Those Divisions with lower or no cost recovery focus on the quality-of-life aspect by providing necessary community services.

  Example: Parks Maintenance

Summary of Expenses and Revenues

- The revenues collected by the Community Recreation Department account for a total of 3.5% ($9,180,646) of revenues collected by the City of Coral Gables.



2024-2025 BUDGET
REVENUES BY SOURCE

2024-2025 - $ $264,339,017

2023-2024 - $ 249,783,024

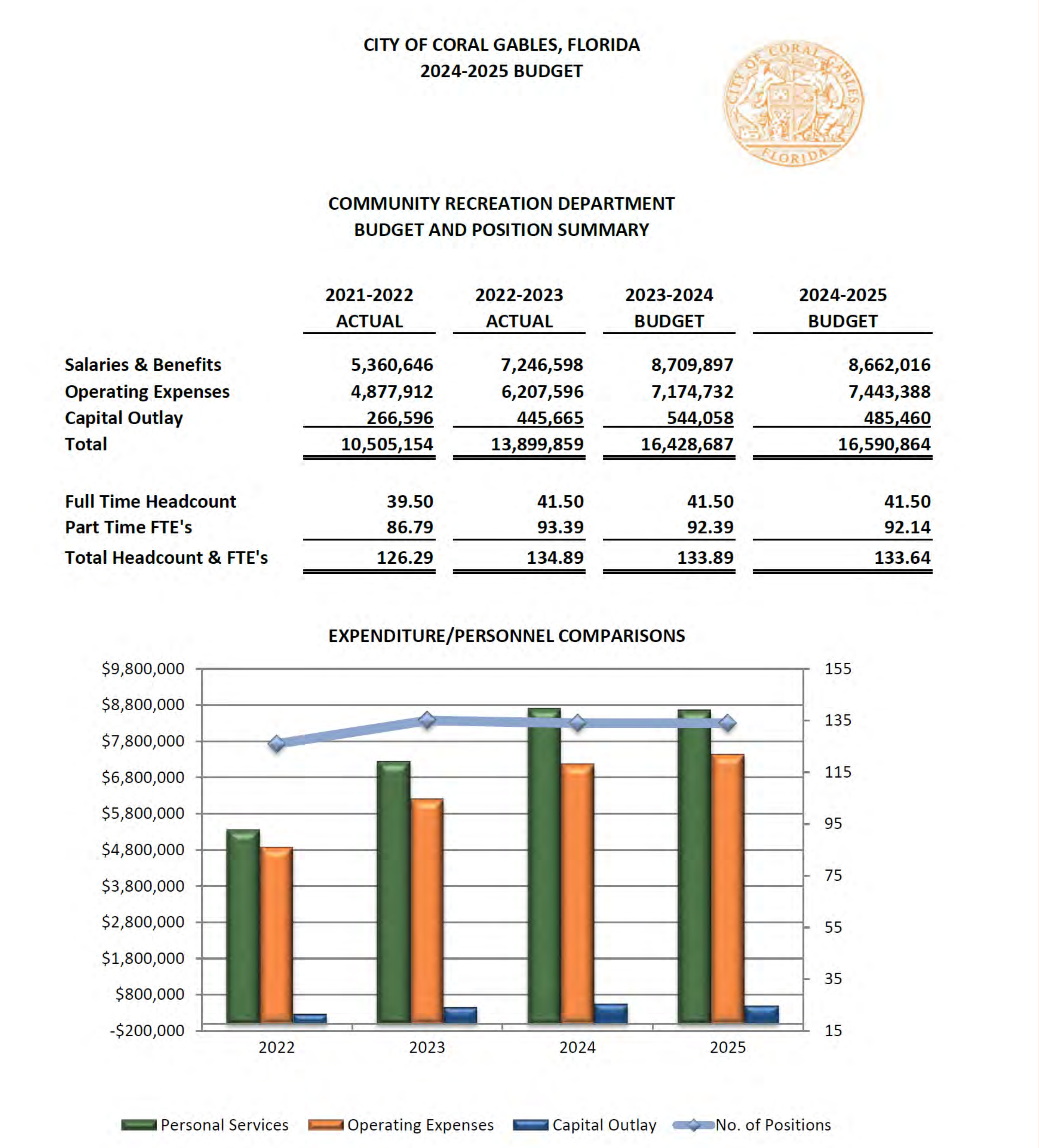
	2023-2024			2024-2025	
		BUDGET	%	BUDGET	%
Property Taxes	$	119,753,649	48.0%	$ 129,944,446	49.2%
Use Charges		48,455,193	19.4%	45,895,624	17.4%
Other Taxes		24,680,000	9.9%	25,959,267	9.8%
Licenses & Permits		13,598,055	5.4%	17,101,125	6.5%
Other		19,112,408	7.7%	17,555,064	6.6%
Intergovernmental Revenues		12,041,319	4.8%	10,372,565	3.9%
Recreation Fees		8,742,400	3.5%	9,180,646	3.5%
Investment Earnings		3,400,000	1.4%	8,330,280	3.2%
Total Revenues	**$**	**249,783,024**	**100.0%**	**$ 264,339,017**	**100.0%**

Cost of Core Services

- The cost of the Department's core services greatly depend on:
  - Salaries for both full and part time personnel & associated benefit costs.
  - General operating expenses
  - Capital outlay for equipment additions or replacement
- The Department measures the head count of full time and part time personnel as they are an essential component and the driving force behind all recreational programs and initiatives.

Cost Recovery

- Department revenues: $9,180,646
- Department budgeted expenditures: $16,590,864
- True departmental operational cost: $7,410,218
- *Averages to a 55% departmental cost recovery model.*



CITY OF CORAL GABLES, FLORIDA
2024-2025 BUDGET

COMMUNITY RECREATION DEPARTMENT
BUDGET AND POSITION SUMMARY

	2021-2022 ACTUAL	2022-2023 ACTUAL	2023-2024 BUDGET	2024-2025 BUDGET
Salaries & Benefits	5,360,646	7,246,598	8,709,897	8,662,016
Operating Expenses	4,877,912	6,207,596	7,174,732	7,443,388
Capital Outlay	266,596	445,665	544,058	485,460
Total	10,505,154	13,899,859	16,428,687	16,590,864
Full Time Headcount	39.50	41.50	41.50	41.50
Part Time FTE's	86.79	93.39	92.39	92.14
Total Headcount & FTE's	126.29	134.89	133.89	133.64

EXPENDITURE/PERSONNEL COMPARISONS

Operating Standards

- The Community Recreation Department adheres to several operating standards:
  - City’s Employee Rules & Guidelines
  - Labor Agreements
  - Administrative and Divisions Specific Policies & Procedures
  - City Code – Find on Municode
  - City Ordinances
  - Any other City, State, or Federal Laws
  - The Department has various employee manuals for each position.
  - Each division has their own set of additional operating standards that govern their specific scope of work or facility type.

OPERATING STANDARDS

- The Community Recreation Department maintains an inventory of:
  - All facilities and neighborhood parks
  - Asset inventory of equipment valued over $1,000
  - The Community Recreation Department also maintains Level of Service (LOS) inventory maps to measure the walkable parks and greenspaces in the City and identify the deficient areas in need of additional land acquisition.

Coral Gables

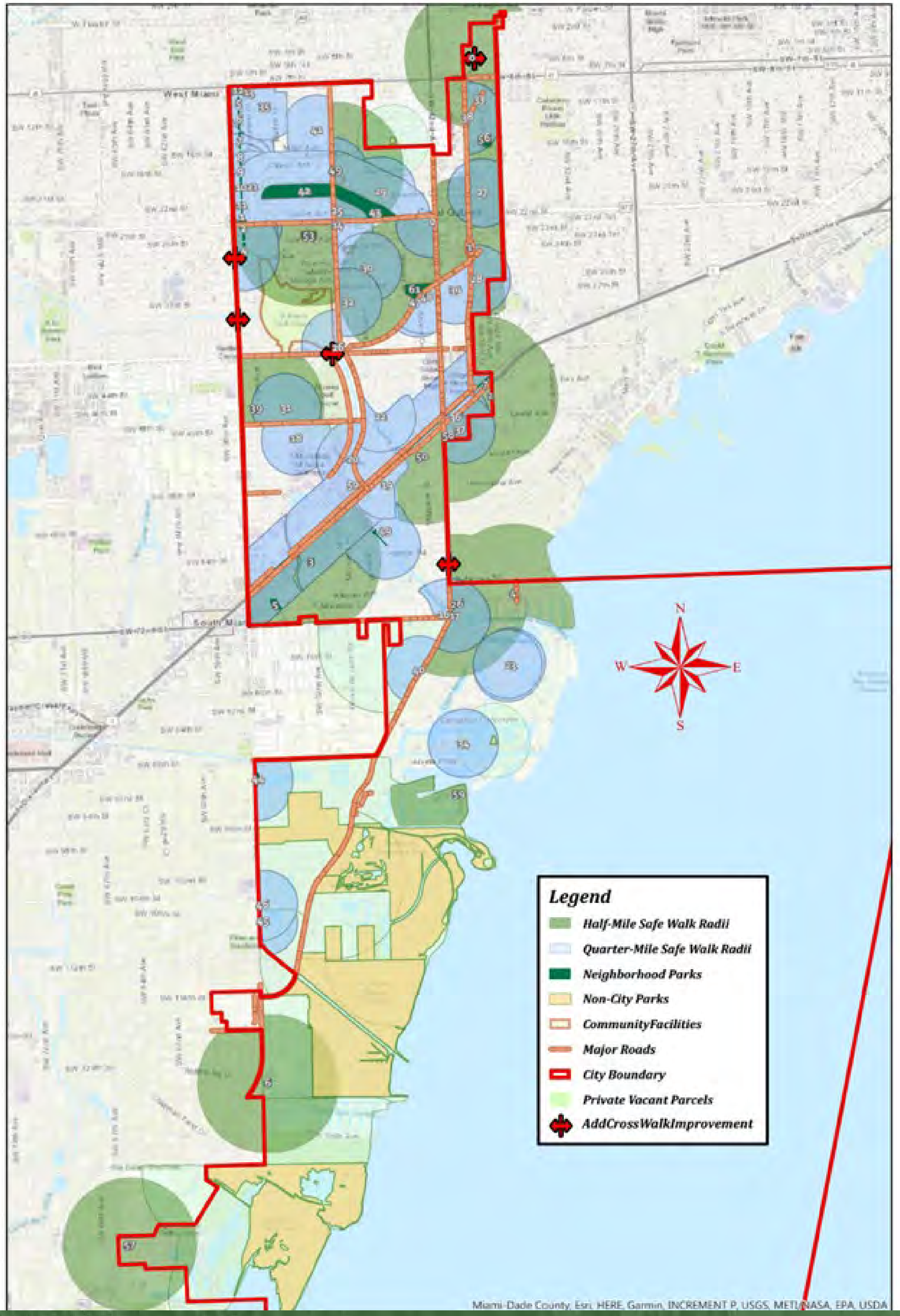
Community Recreation

PARKS & OPEN SPACES AMENITIES

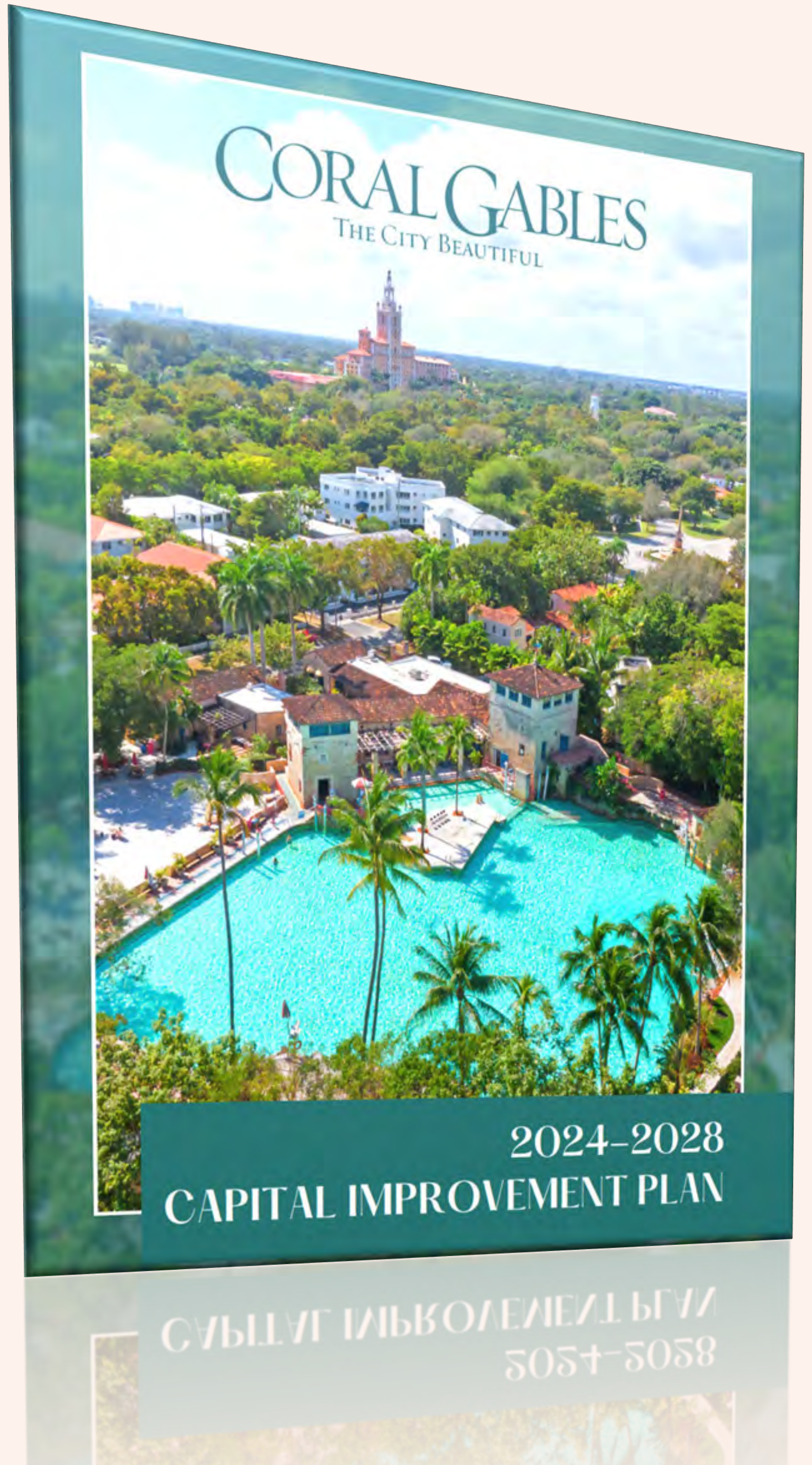
Park	Address	Area Rental Available	Baseball/Softball	Basketball Court	Benches	Bicycle Rack	Community Center	Covered Pavilion	Drinking Fountain	Fitness Gym/Equip.	Golf Course	Gymnastics Gym	Historical Landmark	Multi-Purpose	Parking Area	Paved Trail	Pet-Friendly w/Leash	Pickleball Court	Picnic Tables	Playground	Racquetball Courts	Restrooms	Sidewalks	Soccer Field	Swimming Pool	Tennis Court	Unpaved Trail	Volleyball Court	Waste Receptacles	Water Access	Water Feature
Alcazar Plaza	700 Alcazar Avenue																Y														
Alhambra Water Tower	2000 Alhambra Circle				1								Y				Y														
Balboa Plaza	2405 De Soto Blvd.				1												Y														1
Betsy Adams and the Coral Gables Garden Club Park	4650 Alhambra Circle				4				1							1	Y		2	1									2		1
Blue Road Open Space	757 Blue Road																													Y	
Boy Scouts House - Troop 7	1107 S Greenway Drive			1	6		Y						Y									2	1						2		
Carlos S. Kakouris Park	Campo Sano Ave & Campo Sano Ct.				5																										
Cartagena Park	401 Sunset Drive				4										Y	1	Y						1						1		
Catalonia Park	807 Catalonia Avenue				3				1							1				1			1						2		
City of Coral Gables Biltmore Golf Course	1210 Anastasia Avenue					1			4		1		Y		Y	1						2	13						20	Y	
Coral Bay Park	1590 Campamento Avenue			1	10	1		1	1					1	Y	1	Y		1	2									4		
Coral Gables Adult Activity Center	2 Andalusia Avenue	Y			1		Y		2					1	Y							4	1						3		
Coral Gables Golf & Country Club	997 N. Greenway Dr	Y			1	1	Y		2	1			Y	1	Y				1			2	2		1	6			4		
Coral Gables Merrick House	907 Coral Way				10	1							Y		Y	2			1			1	2						1		1
Coral Gables War Memorial Youth Center	405 University Drive	Y	3	4	12	3	Y	3	8	2		1		1	Y			Y	10	2		10	3	1				2	18		
Country Club Prado	Country Club Prado				1								Y		Y		Y						2								1
Durango Park	3405 Durango Street				2												Y												1		
Enrique "Henry" Cepero Memorial Park	4600 San Amaro Drive				5																										
Ferdinand Park	1500 Coral Way													1			Y														
Fire House Park	San Ignacio Ave & 53rd Court.																														
Fred B. Hartnett Ponce Circle Park	2810 Ponce de Leon Blvd.				21	2											Y						3						5		1
Freedom Plaza	981 E Ponce De Leon Blvd.															1							1								
Galiano Green	95 Almeria Ave					1													1										1		
Gateway Park	142 SW 37th Ave																														
Granada Golf Course	2001 Granada Blvd.				11	1			2		1		Y		Y				1			1				6	1		7		
Granada Park	5151 Granada Blvd.																														
Granada Plaza	Granada Blvd. & Alhambra Circle				3								Y																		1
Ingraham Park	4751 West Ingraham Terr.				30	1			1	1						1	Y		1				1				1		5		1
J. Fritz and Frances Gordon Park	800 Country Club Prado				1								Y		Y		Y														
James H. Smith Park (Corner of Marlin & Banito)	6540 Marlin Drive				4				1							1	Y			1									4		
James T. Barker Park	1047 Venetia Avenue				2				1							1	Y			1			1						2		
Jaycee Park	1230 Hardee Rd.	Y		1	16	1		1	1						Y	1			1	1			1			1			6		1
Lamar Louise Curry Park	2665 De Soto Boulevard				7				1						Y	1	Y						2								
Leucadendra Drive Triangle	331 Leucadendra Drive																														
Lisbon Park	1019 Lisbon Street				5	1			1							1	Y						1								1
Lola B. Walker Pioneers' Park	200 Grand Avenue																						1						1		
Loretta Sheehy Park	410 Sunset Drive				1																						1		1		
MacFarlane Linear Park	100 South Dixie Highway															1															
Maggiore Park	5028 Maggiore Street				3	1			1						Y	1	Y		1	1			3						2		
Majorca Park	937 Majorca Avenue				4				1								Y			1			2						3		
Mall Street Median	Median Mall Street																														
Merrick Park	405 Biltmore Way				4										Y				1										1		
Nellie B. Moore Park	202 Jefferson Dr.				3	1																	2						2		
Orduna Dr-Miller Rd Triangle Park	Corner of Orduna & Miller Road																														
Phillips Park	90 Menores Avenue	Y	1	1	7	1		1	1						Y	1			4	1		2	2	1		2			10		
Pierce Park	101 Oak Avenue				6	1		1	1							1			2	1									4		
Pinewood Cemetery	7401 Erwin Road				12								Y														1		2		
Pittman Park	115 Merrick Way				8	1									Y		Y						3								1
Ponce de Leon Park	1201 Ponce de Leon Blvd.				3										Y		Y						1						1		1
Robert J. Fewell Park	950 Coral Way				7	1										1	Y						1						1		
Rotary Centennial Park	512 Ponce De Leon Blvd.				7										Y	1	Y			1			2						2		
Ruth Bryan Owen Waterway Park	3940 Granada Blvd.				6										Y	1	Y		1				1						1	Y	
Salvadore Dog Run	1120 Andalusia Avenue																Y														
Salvadore Park	1120 Andalusia Avenue	Y			9	2		1	2						Y	1	Y	Y	3	3		2	3						5		
Salvadore Park Tennis Center	1120 Andalusia Avenue				21	1			1						Y				2			2	3			13			12		
Salzedo Park	301 Majorca Avenue																														
San Benito Green	San Benito Ave & El Rado St.																														
San Sebastian Park	130 San Sebastian Avenue																												1		
Sarto Green	241 Sarto Avenue				1																		1						1		
Solano Prado	220 Solano Prado																														
Sunrise Harbor Park	25 E Sunrise Avenue	Y		1	6	1									Y	1			1	2									4		
Toledo and Alava Open Space	Toledo Street and Alava Avenue																														
Venetian Pool	2701 De Soto Blvd.	Y			12	2		1	1				Y		Y	1			12			5	2		1				9		1
Veterans Memorial Park	7700 Old Cutler Rd.																														
William & Leona Cooper Park	4920 Washington Dr.				6											1	Y						1						1		
William H. Kerdyk Biltmore Tennis Center	1150 Anastasia Avenue				4	1			2						Y				2		1	2	2			10			15		
William H. Kerdyk, Jr., and Family Park	6611 Yumuri Street	Y			12	1		1	1	1					Y		Y		2	1			1						9		
Young Park	950 Castile Plaza				5											1	Y														

City of Coral Gables - Walkable Green Space Analysis Citywide

DRAFT



Capital Improvement Needs



CORAL GABLES
THE CITY BEAUTIFUL

2024-2028
CAPITAL IMPROVEMENT PLAN

- Each fiscal year the Community Recreation Department makes its requests to the Commission, City Manager and Budget staff with the requests and identified needs for new land and park acquisitions or new park and facility developments on existing land.
- What is unique to the Capital Improvements Plan for this Department is the 5-Year funding matrix for existing park and facility infrastructure.

CITY OF CORAL GABLES
FISCAL YEAR 2025-2029 FIVE YEAR CAPITAL IMPROVEMENT PLAN
PROJECT SUMMARY & FUNDING SOURCES: COMMUNITY RECREATION REPAIRS/IMPROVEMENTS

COMMUNITY RECREATION PROJECT PARAMETERS

The enhancement and beautification of existing parks and park facilities as well as the development of new parks and park facilities.

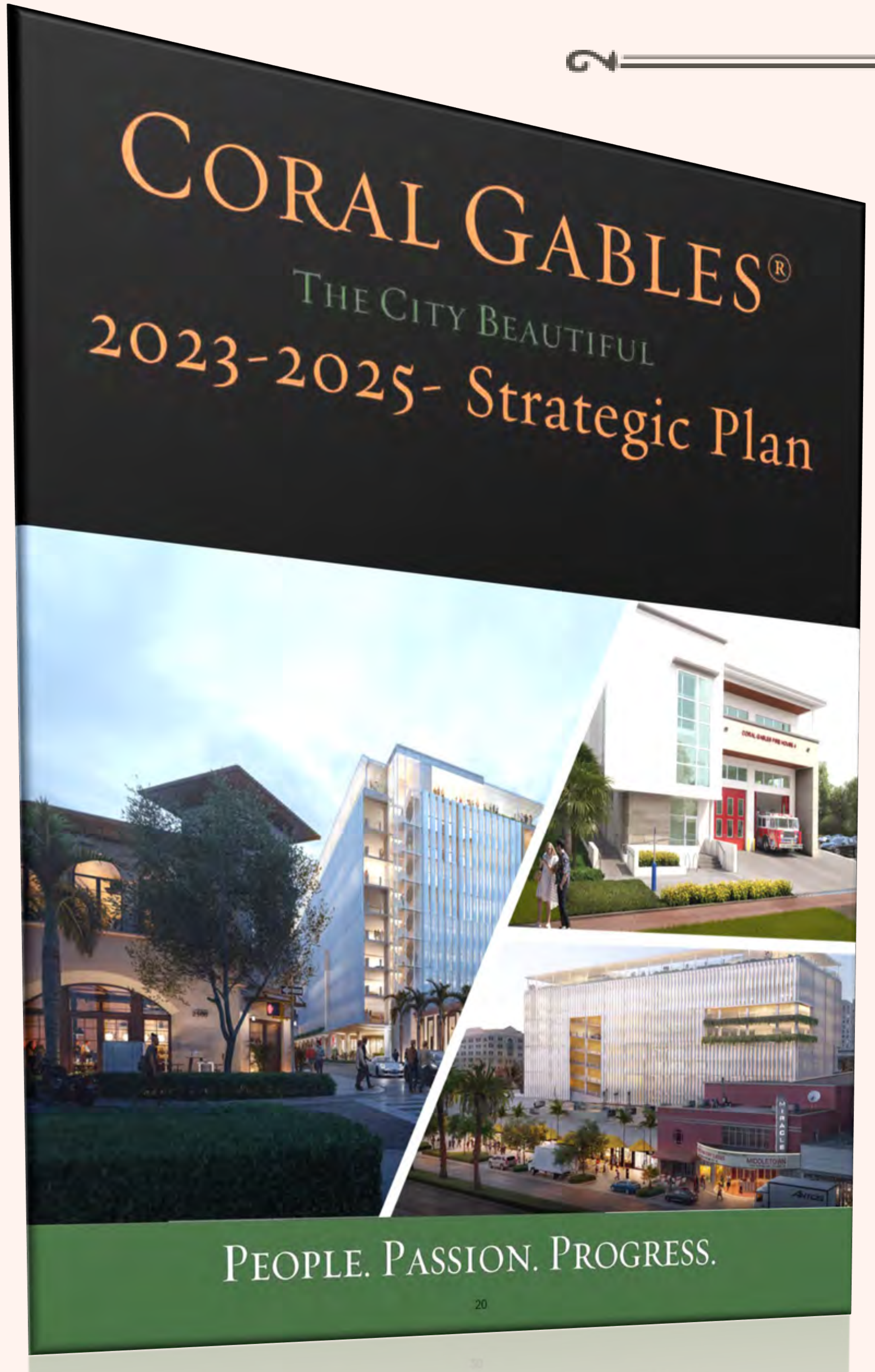
COMMUNITY RECREATION PROJECTS BY YEAR

PAGE #	PROJECT NAME	FIVE-YEAR ESTIMATE								FIVE-YEAR PROJECT TOTAL
		2025				2026	2027	2028	2029	
		PR YR AVAIL	OPEN P.O.	NEW	TOTAL					
102	Purchase of Land	$ 3,818,148	$ -	$ 1,373,502	$ 5,191,650	$ 500,000	$ 500,000	$ 500,000	$ 500,000	$ 7,191,650
105	Fred B. Hartnett/Ponce Circle Park Phase 1/Phase 2	5,298,488	82,680	-	5,381,168	-	3,696,000	-	-	9,077,168
109	Development of Neighborhood Parks	50,000	-	-	50,000	-	-	-	-	50,000
110	Betsy Adams Park Enhancements	-	-	-	-					-
111	Catalonia Park Enhancements	-	-	-	-	594,608	-	-	-	594,608
112	Durango Parks Enhancements	-	-	-	-	717,173	-	-	-	717,173
113	Hammock Oaks Park	-	-	-	-	549,548	-	-	-	549,548
115	Merrick Park Improvements	-	-	-	-	-	-	1,350,000	-	1,350,000
117	William and Leona Cooper and Nellie B. Moore Park Enhancements	553,422	90,392	127,629	771,443	350,000	-	-	-	1,121,443
119	Orduna Park Enhancement	-	-	-	-	51,500	472,748	-	-	524,248
120	Salzedo Park Development	-	-	-	-	128,250	1,201,654	-	-	1,329,904
123	Mayor Dorothy H. Thomson Park	1,074,585	46,513	145,291	1,266,389	-	-	-	-	1,266,389
124	San Sebastian Park Enhancements	-	-	-	-	91,500	538,748	-	-	630,248
127	Mar Street-Play Street	-	-	-	-	-	-	200,000	-	200,000
129	Manatee Overlook	-	-	-	-	-	-	200,000	-	200,000
130	Youth Center Pickleball Court Installation Plan	-	-	-	-	-	-	-	-	-
131	Citywide Pickleball Court Installation Plan	-	-	500,000	500,000	-	-	-	-	500,000
132	Coral Bay Park Renovation & Enhancement	-	-	-	-	350,000	541,500	230,000	3,061,823	4,183,323
133	North Entrance Park Development	-	-	-	-	82,500	315,000	250,000	354,813	1,002,313
134	Rotary Park Enhancement	91,255	121,545	-	212,800	116,792	-	-	-	329,592
135	The James and Sallye Jude Park Renovation and Enhancement	-	-	-	-	1,005,698	1,200,000	1,800,000	-	4,005,698
136	Parks & Recreation Major Repairs	5,976,699	465,245	1,854,641	8,296,585	1,942,500	3,554,500	2,205,000	2,180,000	18,178,585
141	Coral Gables Country Club Improvements	541,948	78,953	657,646	1,278,547	2,150,000	2,650,000	2,650,000	2,650,000	11,378,547
143	Granada Golf Course Diner Renovations	98,669	141,822	-	240,491	-	-	-	-	240,491
144	Granada Golf Course Improvements	290,092	11,127	160,000	461,219	300,000	300,000	300,000	100,000	1,461,219
147	Salvadore Park Improvements	1,000	-	-	1,000	-	-	-	-	1,000
148	Youth Center Improvements	259,010	-	-	259,010	-	-	-	-	259,010
149	Coral Gables Senior High Park	-	-	50,000	50,000	-	-	-	-	50,000
151	Blue Road Open Space Improvements	1,315,311	32,242	-	1,347,553	-	-	-	-	1,347,553
153	Jaycee Park Enhancements	-	-	-	-	250,000	500,000	1,025,875	-	1,775,875
155	Phillips Park Renovation and Enhancement	3,948,646	702,856	4,787,500	9,439,002	-	-	-	-	9,439,002
	TOTAL	$ 23,317,273	$ 1,773,375	$ 9,656,209	$ 34,746,857	$ 9,180,069	$ 15,470,150	$ 10,710,875	$ 8,846,636	$ 78,954,587

CITY OF CORAL GABLES
COMMUNITY RECREATION MAJOR REPAIR PROJECTS BY YEAR

PROJECT NAME	FIVE-YEAR ESTIMATE								FIVE-YEAR PROJECT TOTAL
	2025				2026	2027	2028	2029	
	PR YR AVAIL	OPEN P.O.	NEW	TOTAL					
Artificial Turf Safety Surfacing Replacement & Additions	$ 300,000	$ -	$ 100,000	$ 400,000	$ 100,000	$ -	$ 100,000	$ 100,000	$ 700,000
Blue Road Open Space Renovation	1,073,077	32,242	136,683	1,242,002	-	-	-	-	1,242,002
Cepero Park Improvements - Phase 2	225,000	-	-	225,000	-	-	-	-	225,000
Coral Bay Playground	-	-	-	-	-	750,000	-	-	750,000
Creation of Dog Park at Gables Station	-	7,623	-	7,623	-	-	-	-	7,623
Fitness Trails	34,371	-	-	34,371	-	-	100,000	100,000	234,371
Granada Golf Course Groundwater Diversion	1,250	2,000	-	3,250	-	-	-	-	3,250
Granada Golf Maintenance Shop Renovation	301,999	-	300,000	601,999	300,000	300,000	-	-	1,201,999
Granada Golf Course Shelter Improvements	224,898	-	100,000	324,898	-	-	-	-	324,898
Holiday Tree Purchase ✓	6,125	-	-	6,125	-	-	-	-	6,125
Ingraham Park Fitness Equipment	-	-	-	-	250,000	-	-	-	250,000
Kerdyk Family Park Playground Expansion ✓	12,116	-	-	12,116	-	-	200,000	200,000	412,116
Kerdyk Family Park Trail Renovation ✓	4,439	-	-	4,439	-	-	-	-	4,439
Lighting for Park Facilities	150,000	-	50,000	200,000	-	-	100,000	100,000	400,000
Lightning Protection System for Facilities	61,000	-	50,000	111,000	-	-	50,000	50,000	211,000
P&R Facilities Surveillance Systems	106,351	-	50,000	156,351	42,500	42,500	85,000	85,000	411,351
Park Basketball and Tennis Court Renovations ✓	119,000	-	-	119,000	-	-	20,000	20,000	159,000
Park Furnishings	146,999	-	75,000	221,999	75,000	75,000	75,000	75,000	521,999
Park Facilities Furnishings - Interiors	-	-	67,958	67,958	100,000	100,000	100,000	100,000	467,958
Pierce Park Renovation	67,326	-	-	67,326	-	-	-	-	67,326
Resurfacing of Clay Courts ✓	-	-	-	-	-	-	-	-	-
Rotary Park Improvements	567,735	-	200,000	767,735	531,000	531,000	-	-	1,829,735
Ruth Bryan Owen Waterway Park Renovation	400,000	-	200,000	600,000	-	-	100,000	100,000	800,000
Dog Park Artificial Turf Installation	-	-	-	-	-	-	-	-	-
Salvadore Park Dog Designated Areas	-	101	-	101	-	-	-	-	101
Salvadore Park Tennis Facility Renovation	-	-	-	-	-	-	-	-	-
Salvadore Park Playground Expansion	56,094	771	-	56,865	-	-	-	-	56,865
Salvadore Park Playground Replacement ✓	3,624	-	-	3,624	-	-	-	-	3,624
Salvadore Park Tennis Pro Shop Renovation	1,000	-	-	1,000	-	-	-	-	1,000
Salvadore Park Tennis Shade Addition	25,398	-	-	25,398	-	-	-	-	25,398
Shade Structure Repairs & Additions	198,043	-	50,000	248,043	-	100,000	100,000	100,000	548,043
Sunrise Harbor Playground Replacement	-	-	-	-	369,000	881,000	-	-	1,250,000
Venetian Pool Improvements	108,197	-	300,000	408,197	100,000	100,000	100,000	100,000	808,197
Venetian Pool Concession Stand Renovation	200,678	93,050	-	293,728	-	-	-	-	293,728
Venetian Pool Phase 6	98,008	1,425	-	99,433	-	-	200,000	200,000	499,433
Venetian Pool Pump & Utilities Renovation	824,650	62,059	-	886,709	-	-	50,000	50,000	986,709
Youth Center Amenities Improvements	1,001	-	-	1,001	-	200,000	200,000	200,000	601,001
Youth Center Courtyard Improvements	29,151	-	-	29,151	-	400,000	400,000	400,000	1,229,151
Youth Center Field Doors & Gates	100,000	-	-	100,000	-	-	-	-	100,000
Youth Center Fitness Center Renovations	77,581	-	-	77,581	-	-	-	-	77,581
Youth Center Indoor Gym Renovations	105,000	-	-	105,000	-	-	-	-	105,000
Youth Center Intercom & P.A. Replacement	60,000	-	-	60,000	-	-	-	-	60,000
Youth Center Interior Renovations ✓	46,925	-	-	46,925	-	-	100,000	100,000	246,925
Youth Center Master Plan ✓	-	-	-	-	-	-	-	-	-
Youth Center Paint Exterior Building	2,846	-	-	2,846	-	-	-	-	2,846
Youth Center Phase 1 Improvements ✓	21,780	-	-	21,780	-	-	-	-	21,780
Youth Center Structural Improvements ✓	83,243	265,974	-	349,217	-	-	50,000	50,000	449,217
Youth Center & Grounds Improvements ✓	5,612	-	-	5,612	-	-	-	-	5,612
Youth Center Field Resod & Irrigation ✓	101,182	-	100,000	201,182	-	-	-	-	201,182
Water Fountain Replacement	-	-	50,000	50,000	50,000	50,000	50,000	50,000	250,000
Well Identification Program	25,000	-	25,000	50,000	25,000	25,000	25,000	-	125,000
Unassigned	-	-	-	-	-	-	-	-	-
TOTAL	$ 5,976,699	$ 465,245	$ 1,854,641	$ 8,296,585	$ 1,942,500	$ 3,554,500	$ 2,205,000	$ 2,180,000	$ 18,178,585

City of Coral Gables Strategic Plan



Coral Gables®

The City Beautiful

2023-2025- Strategic Plan

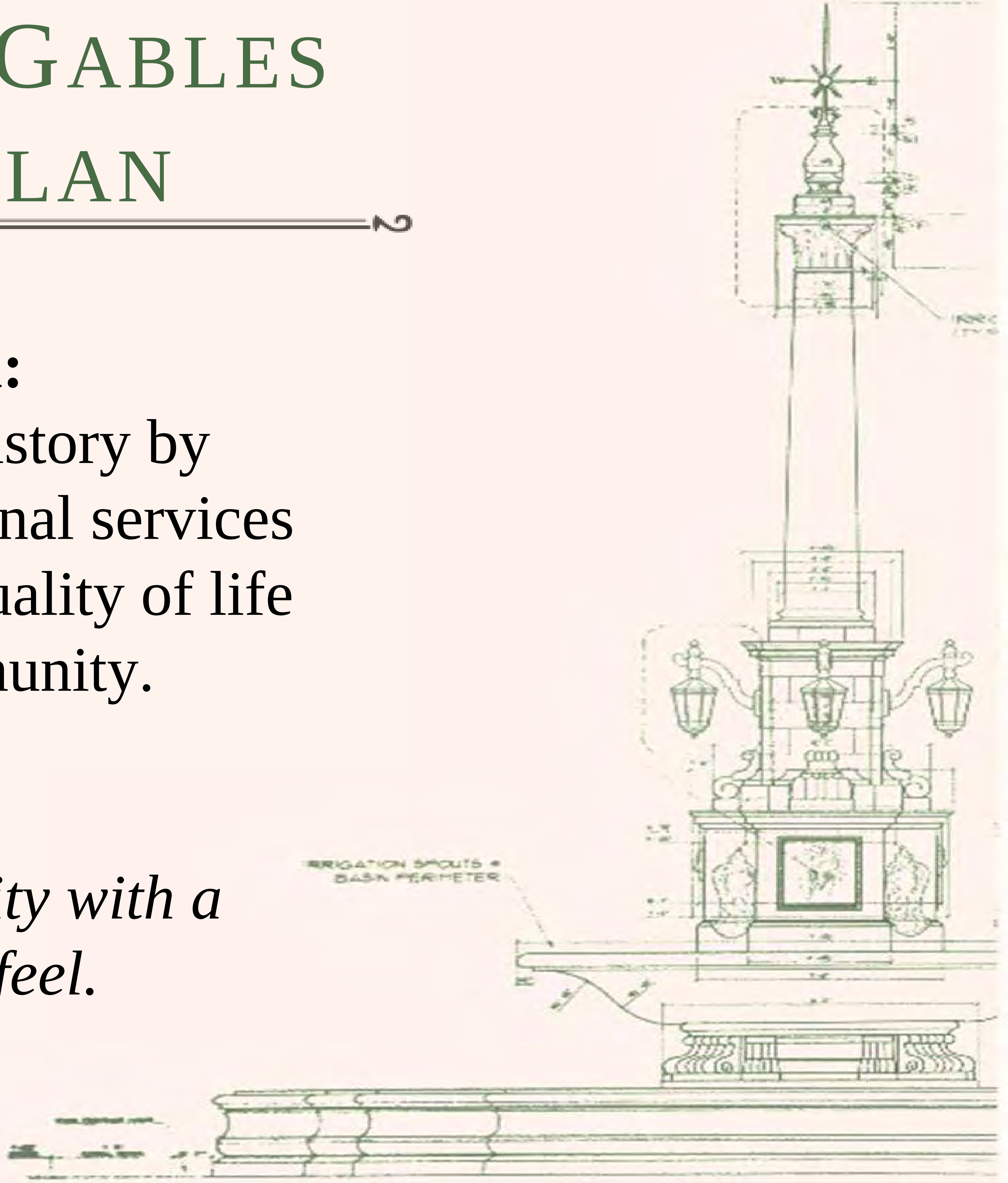
People. Passion. Progress.

Mission:

To honor our history by providing exceptional services that enhance the quality of life for our community.

Vision:

A world-class city with a hometown feel.



City of Coral Gables Strategic Plan

Values:

Governance with integrity- making ethical and wise choices with guided thought and transparency

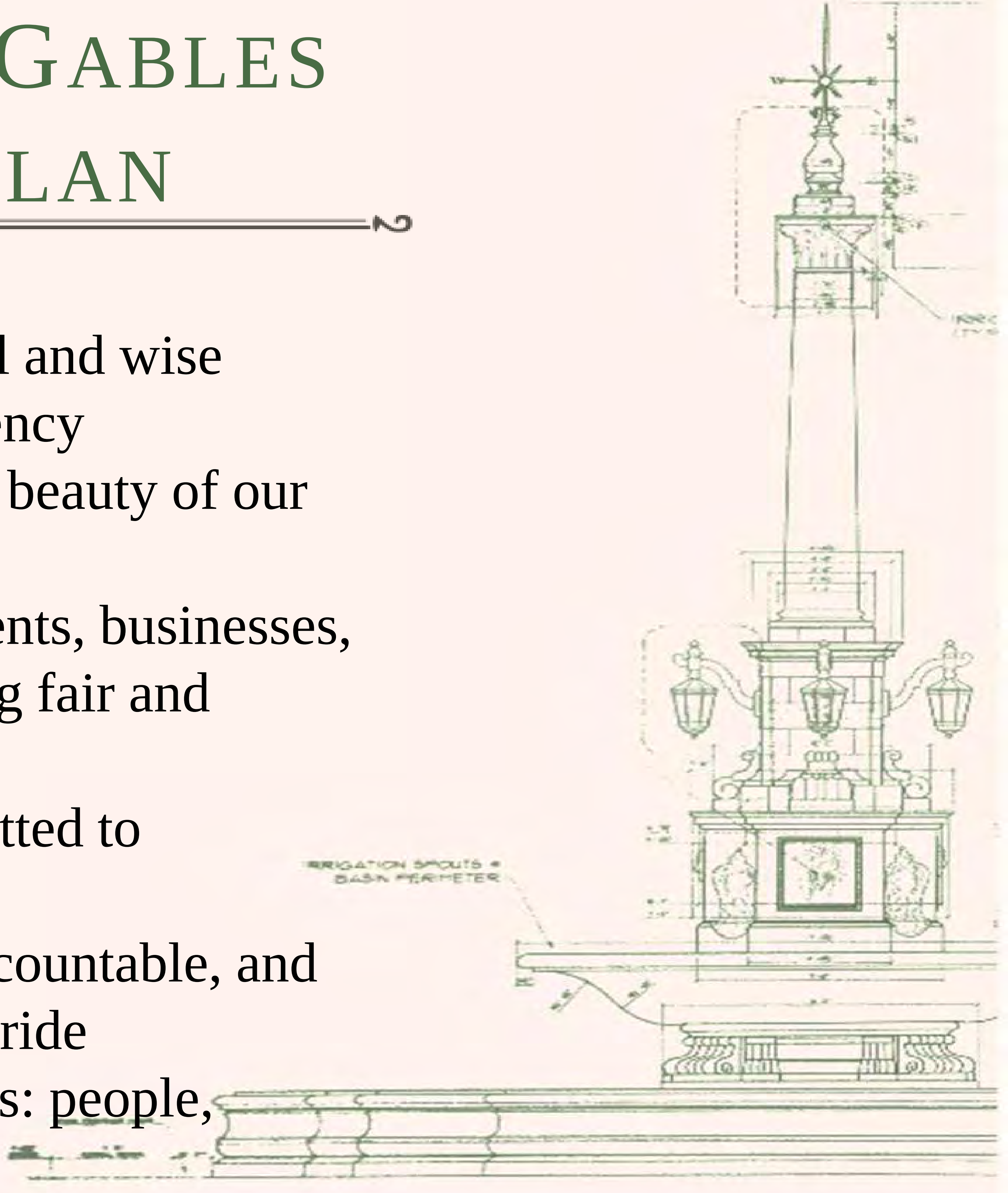
Aesthetics - preserving and enhancing the beauty of our city

Balanced - considering all interests: residents, businesses, and workforce; celebrating diversity; being fair and equitable

Learning - inspired by our history, committed to excellence and innovation for our future

Exceptional service - being accessible, accountable, and respectful - exceeding expectations with pride

Sustainability- stewardship of all resources: people, finances, facilities, and the environment



Trivia Question #4

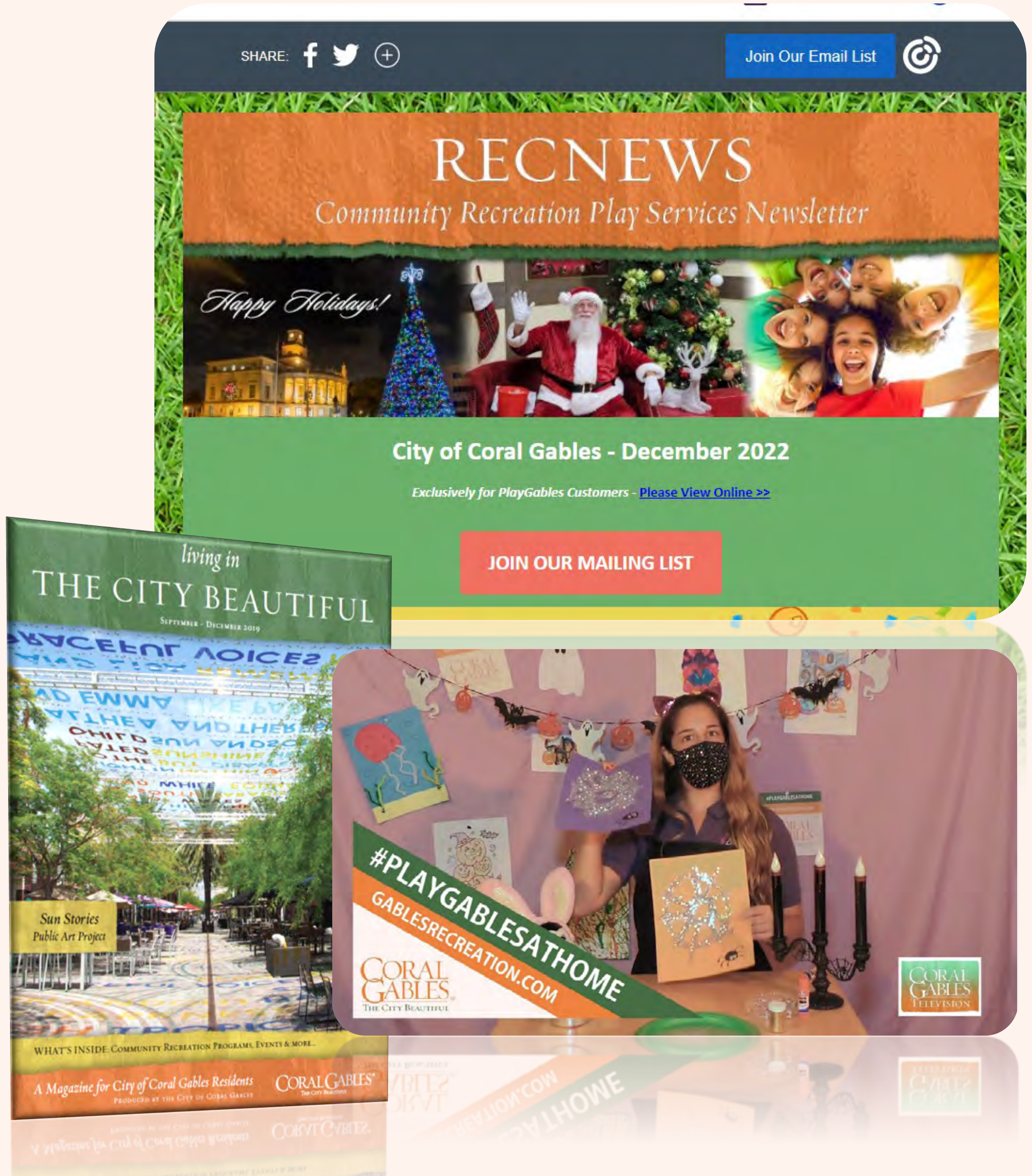
WHAT YEAR WAS THE CITY OF CORAL GABLES INCORPORATED?

Correct Answer to Question #4

1925

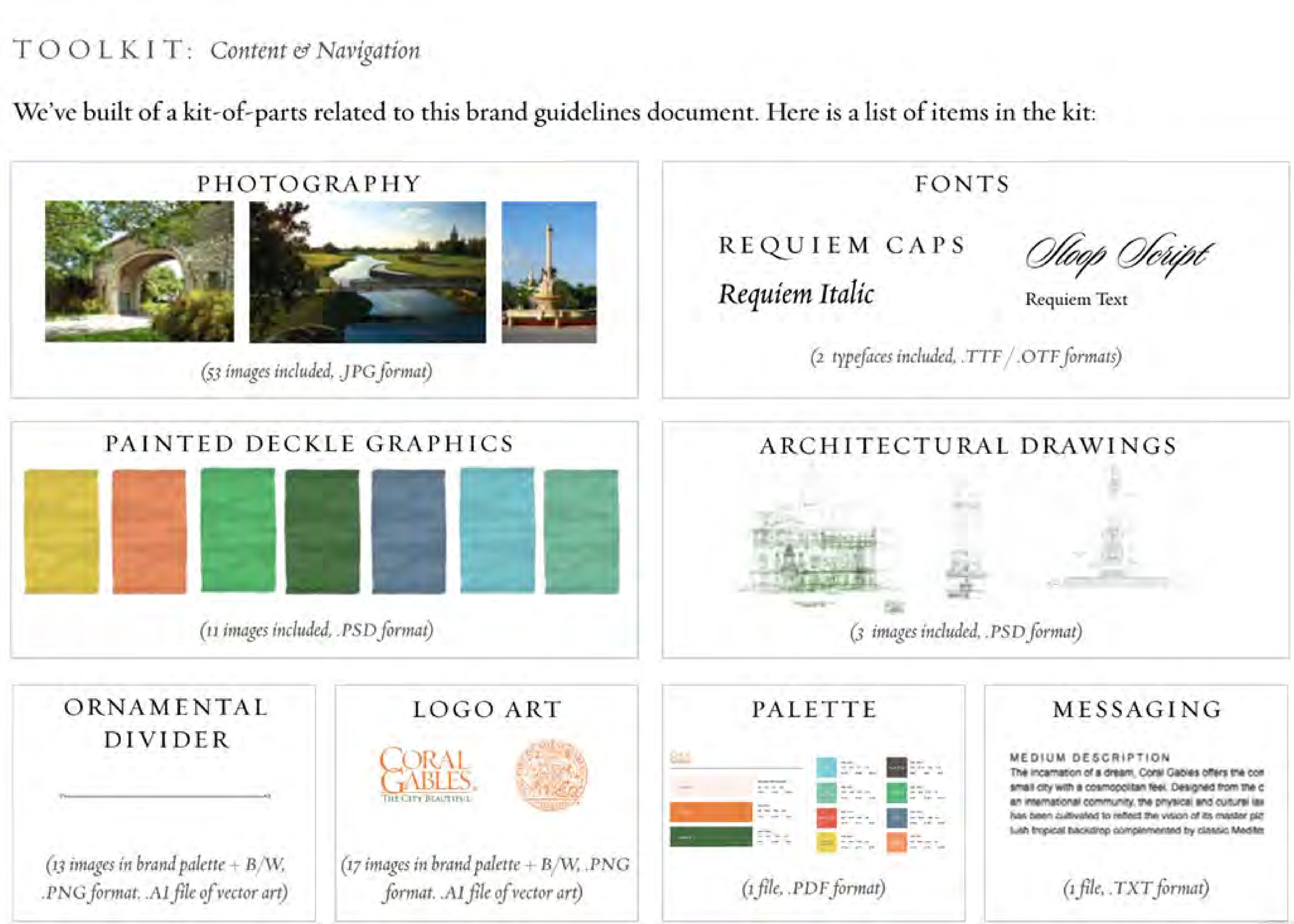
Implementation Strategies

Marketing Strategies



- Print Media
  - Posters, Flyers, Brochures & Door Hangers
- Multimedia & Social Media
  - Newsletter - E-NEWS & RecNews
  - Facebook – various pages
  - Instagram - various pages
  - Nextdoor – various pages
  - Twitter – City page
  - LinkedIn – City page
  - YouTube Channel
  - Coral Gables App

Branding Guidelines



TOOLKIT: *Content & Navigation*

We've built of a kit-of-parts related to this brand guidelines document. Here is a list of items in the kit:

PHOTOGRAPHY

(53 images included, .JPG format)

FONTS

REQUIEM CAPS

Requiem Italic

Sloop Script

Requiem Text

(2 typefaces included, .TTF / .OTF formats)

PAINTED DECKLE GRAPHICS

(11 images included, .PSD format)

ARCHITECTURAL DRAWINGS

(3 images included, .PSD format)

ORNAMENTAL DIVIDER

(13 images in brand palette + B/W, .PNG format. .AI file of vector art)

LOGO ART

(17 images in brand palette + B/W, .PNG format. .AI file of vector art)

PALETTE

(1 file, .PDF format)

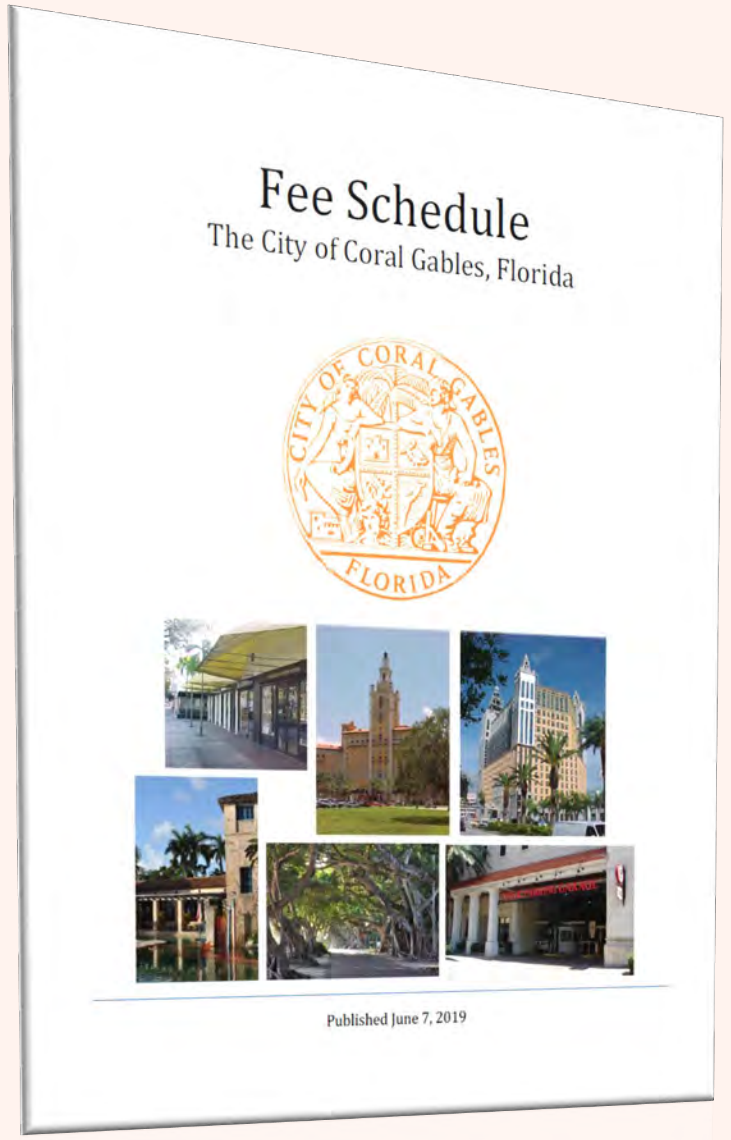
MESSAGING

MEDIUM DESCRIPTION

The incarnation of a dream, Coral Gables offers the con
small city with a cosmopolitan feel. Designed from the c
an international community, the physical and cultural las
has been cultivated to reflect the vision of its master pla
lush tropical backdrop complemented by classic Medite

(1 file, .TXT format)

Pricing Strategies

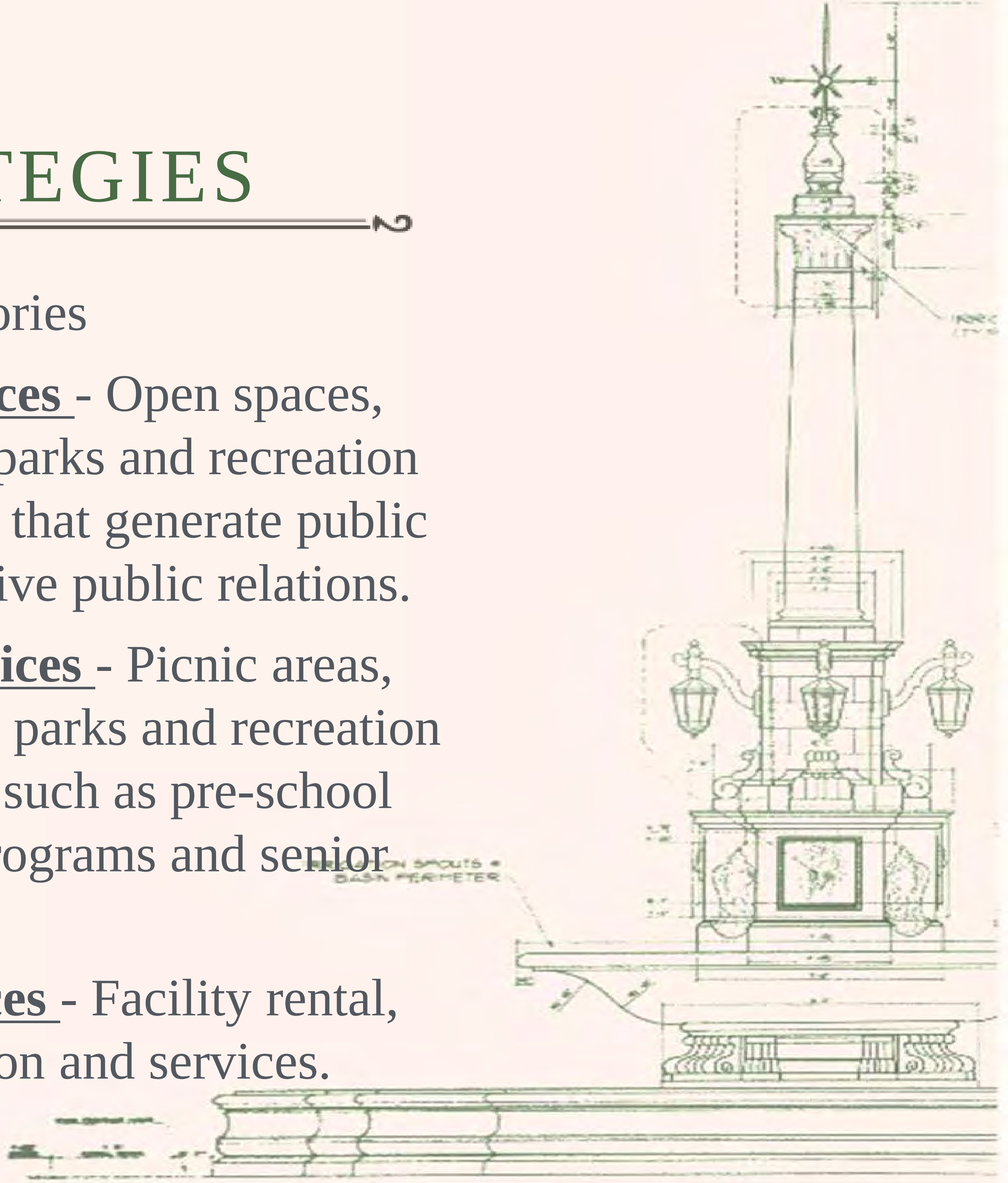


Fee Schedule

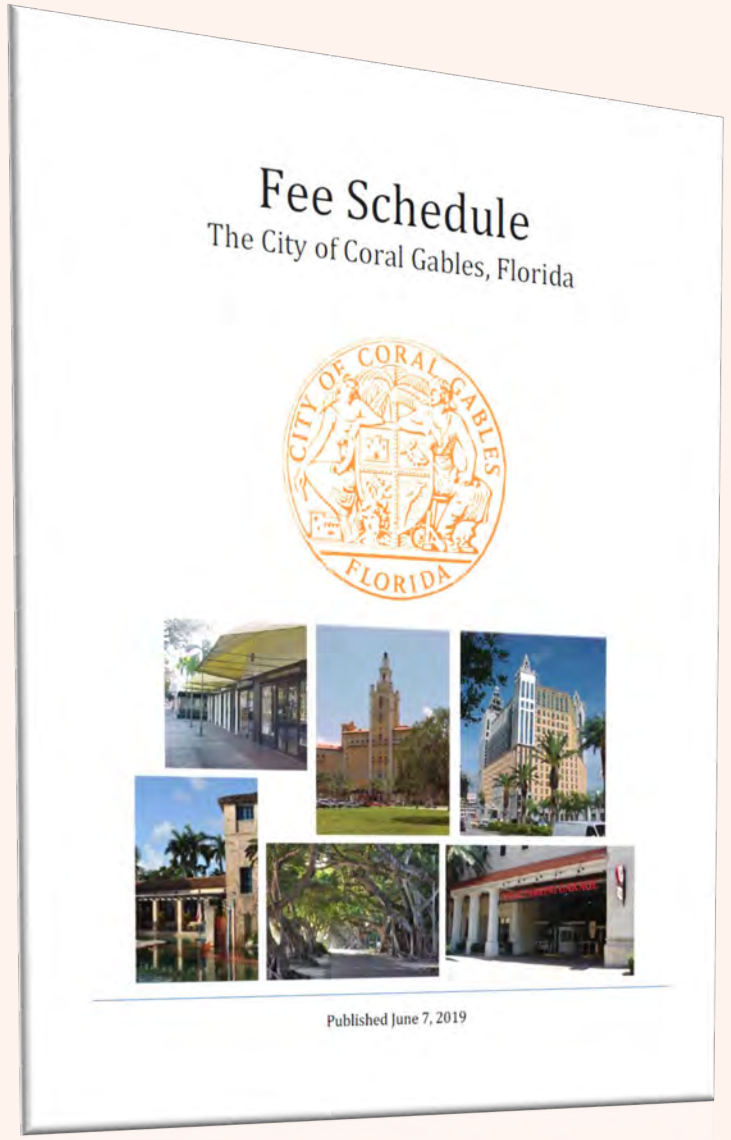
The City of Coral Gables, Florida

Published June 7, 2019

- Fee Assessment Categories
  - **Public Based Services** - Open spaces, playgrounds, trails, parks and recreation sponsored programs that generate public awareness and positive public relations.
  - **Private Based Services** - Picnic areas, tennis, aquatics, and parks and recreation sponsored activities such as pre-school instruction, youth programs and senior citizen activities.
  - **Merit Based Services** - Facility rental, specialized instruction and services.



PRICING STRATEGIES

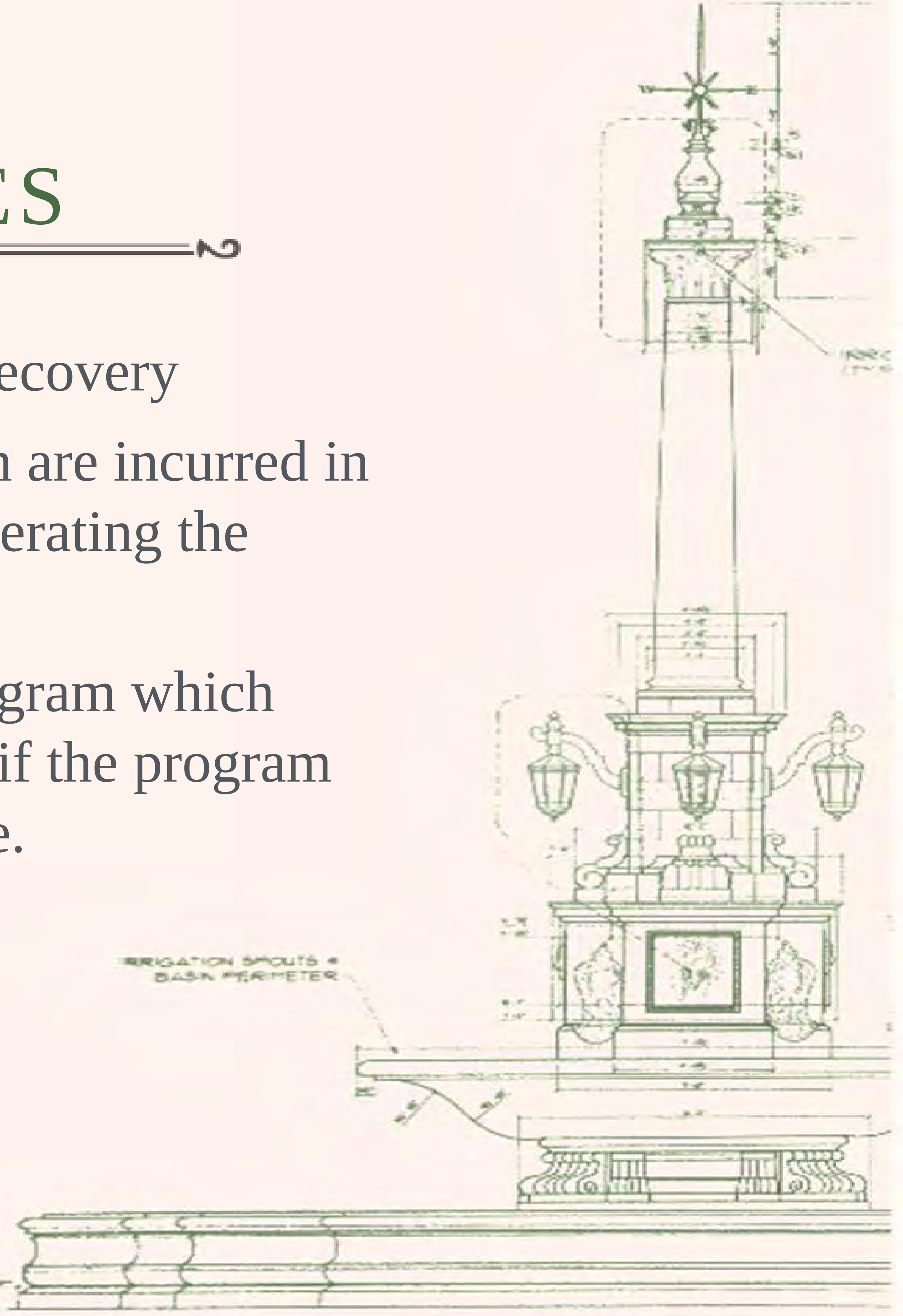


Fee Schedule

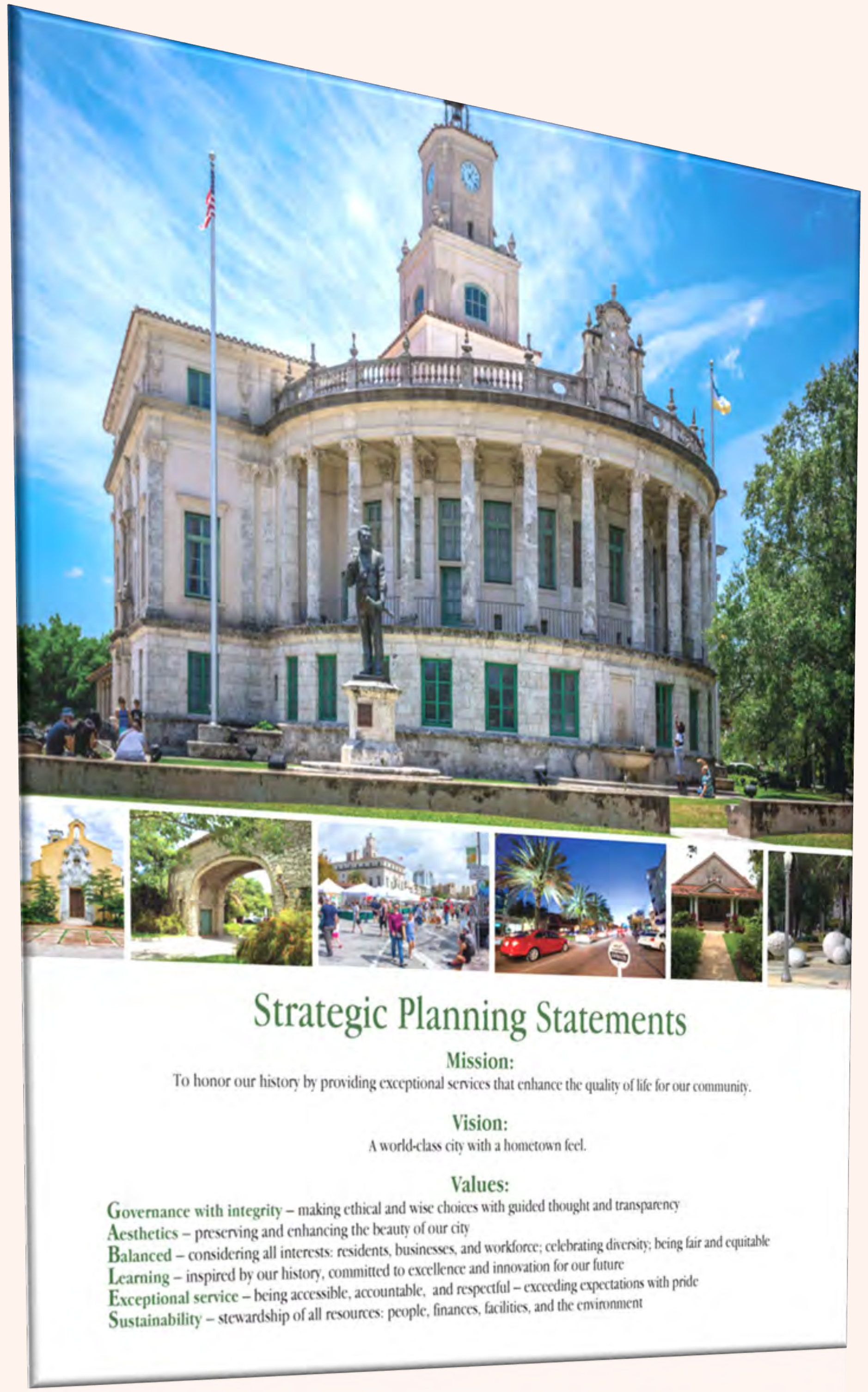
The City of Coral Gables, Florida

Published June 7, 2019

- Pricing Determinants for Cost Recovery
  - Direct Costs - expenses which are incurred in conducting the program or operating the program or activity
  - Fixed Costs – costs to the program which would be incurred regardless if the program or activity where to take place.
- User Fees By Type
  - Member
  - Resident
  - Non-Resident
- 5 Year Fee Plan – 2.5% increase



Organizational Needs



Strategic Planning Statements

Mission:

To honor our history by providing exceptional services that enhance the quality of life for our community.

Vision:

A world-class city with a hometown feel.

Values:

Governance with integrity – making ethical and wise choices with guided thought and transparency
Aesthetics – preserving and enhancing the beauty of our city
Balanced – considering all interests: residents, businesses, and workforce; celebrating diversity; being fair and equitable
Learning – inspired by our history, committed to excellence and innovation for our future
Exceptional service – being accessible, accountable, and respectful – exceeding expectations with pride
Sustainability – stewardship of all resources: people, finances, facilities, and the environment

- Budget Input
  - 100% Budget Adjustments
  - New Need Submission Packages
  - New Need CIP Packages
  - Budget Cut Exercise Scenarios
- Implementation Priorities
  - Commission mandates
  - City Manager mandates
  - Ongoing maintenance
  - Items associated with the Strategic Plan
  - Community driven
  - Revenue driven

15 Minute Break

CORAL GABLES
THE CITY BEAUTIFUL

Leadership Workshop

Leadership Training

Organizational Commitment

What Does It Mean to Be “Committed”?

For You or Your Team?

Organizational Commitment

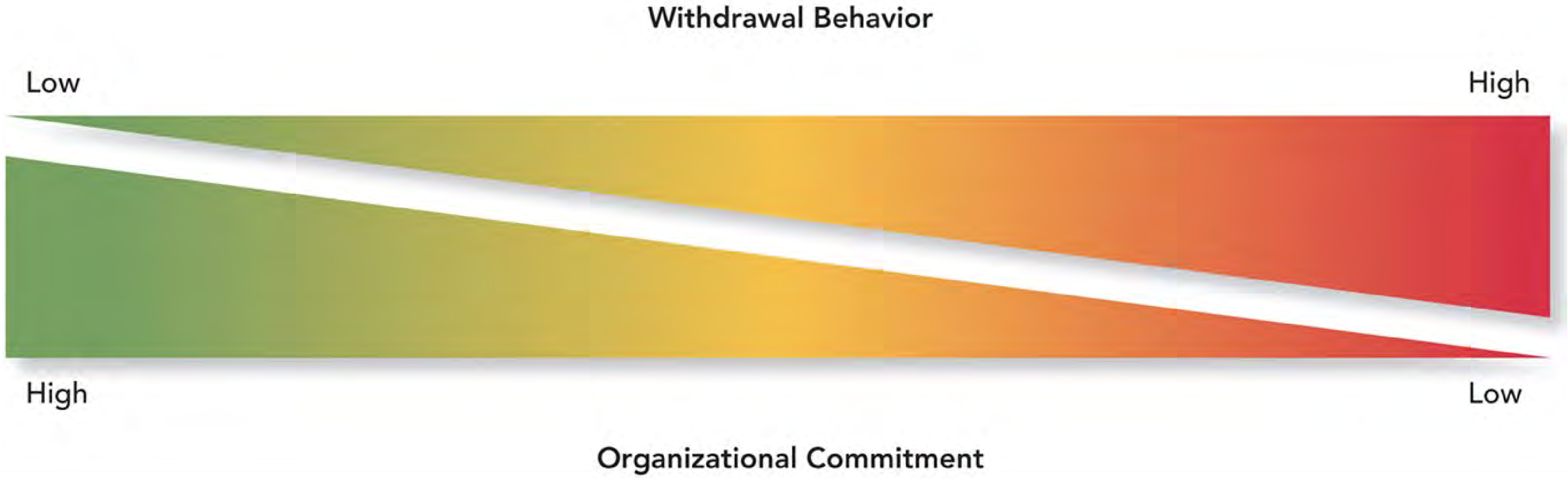
Organizational commitment is the desire of an employee to remain a member of an organization.

The desire may be based on want, need, or feeling of obligation

Consider this scenario:

- You’ve worked at your current employer for five years and have recently been approached by a competing organization.
- What would cause you to stay?
- Do those reasons fit into different kinds of categories?

Organizational Commitment and Employee Withdrawal



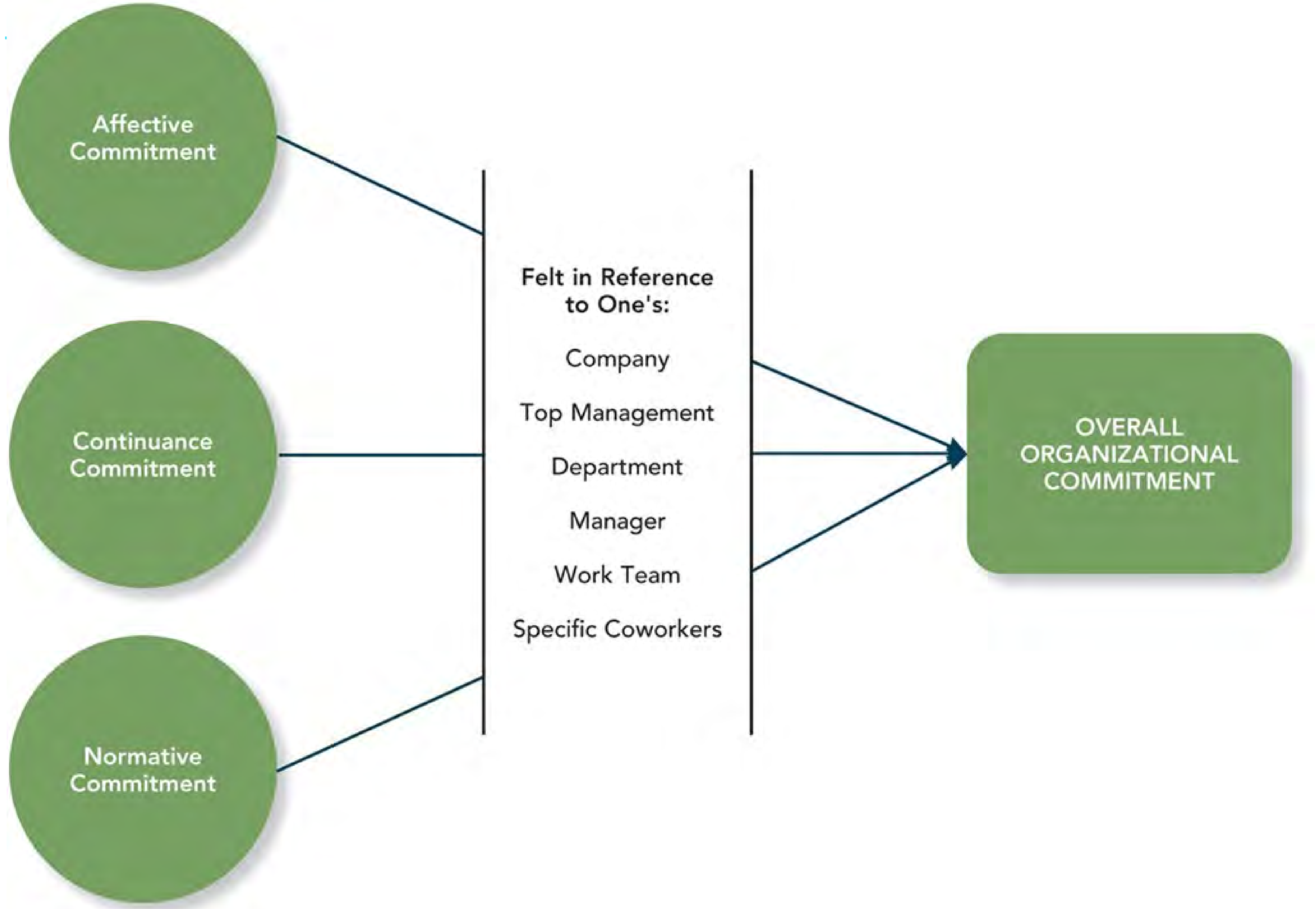
Most people are in the yellow part of this diagram: around 50% commitment and 50% withdrawal. Of course, it’s worth noting that no organization would ever want their employees to be 100-0. That would be a recipe for burnout, along with other problems.

The Three Types of Organizational Commitment

What Makes Someone Stay with their Current Organization?

AFFECTIVE COMMITMENT (EMOTION-BASED)	CONTINUANCE COMMITMENT (COST-BASED)	NORMATIVE COMMITMENT (OBLIGATION-BASED)
Some of my best friends work in my office … I'd miss them if I left.	I'm due for a promotion soon … Will I advance as quickly at the new company?	My boss has invested so much time in me, mentoring me, training me, showing me the ropes.
I really like the atmosphere at my current job … It's fun and relaxed.	My salary and benefits get us a nice house in our town … The cost of living is higher in this new area.	My organization gave me my start … It hired me when others thought I wasn't qualified.
My current job duties are very rewarding … I enjoy coming to work each morning.	The school system is good here and my partner has a good job … We've really put down roots where we are.	My employer has helped me out of a jam on a number of occasions … How could I leave now?
Staying because you ***want*** to.	Staying because you ***need*** to.	Staying because you ***ought*** to.

Drivers of Overall Organizational Commitment



Affective Commitment

Continuance Commitment

Normative Commitment

Felt in Reference to One's:

Company

Top Management

Department

Manager

Work Team

Specific Coworkers

OVERALL ORGANIZATIONAL COMMITMENT

Affective Commitment

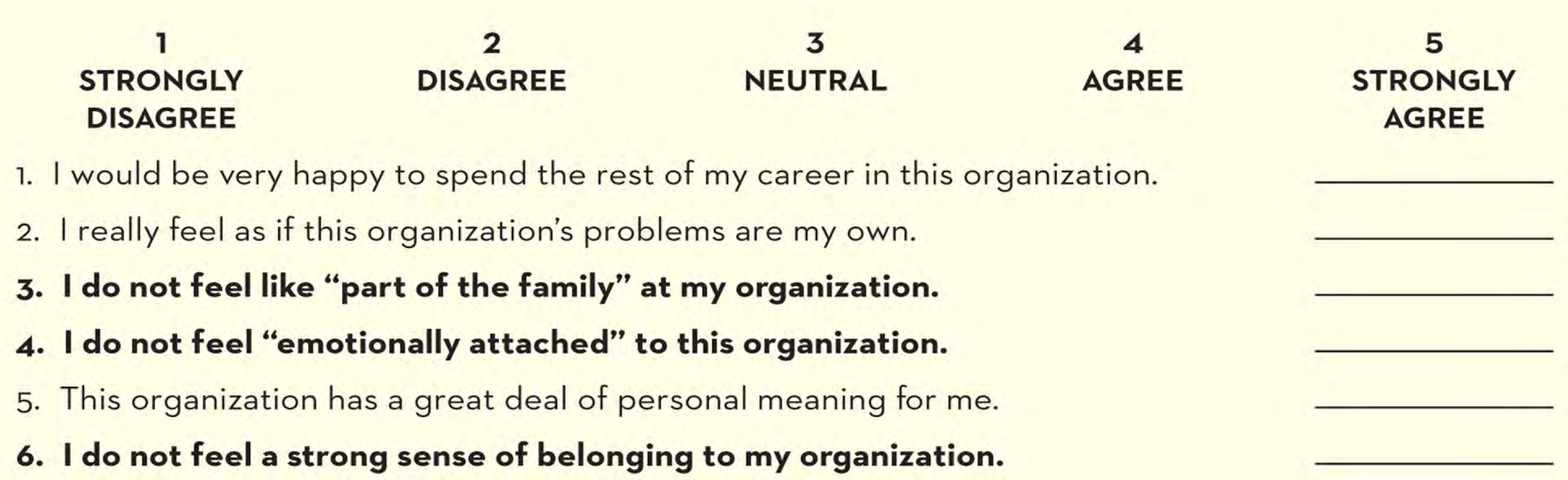
- A desire on the part of an employee to remain a member of an organization because of an emotional attachment to, and involvement with, that organization.

- You stay because you want to.

- What would you feel if you left anyway?

- You'd feel sad. So affectively committed people stay, as much as anything, to avoid feeling sad.

Assessment On Affective Commitment



1	2	3	4	5
STRONGLY DISAGREE	DISAGREE	NEUTRAL	AGREE	STRONGLY AGREE

1. I would be very happy to spend the rest of my career in this organization. ____________

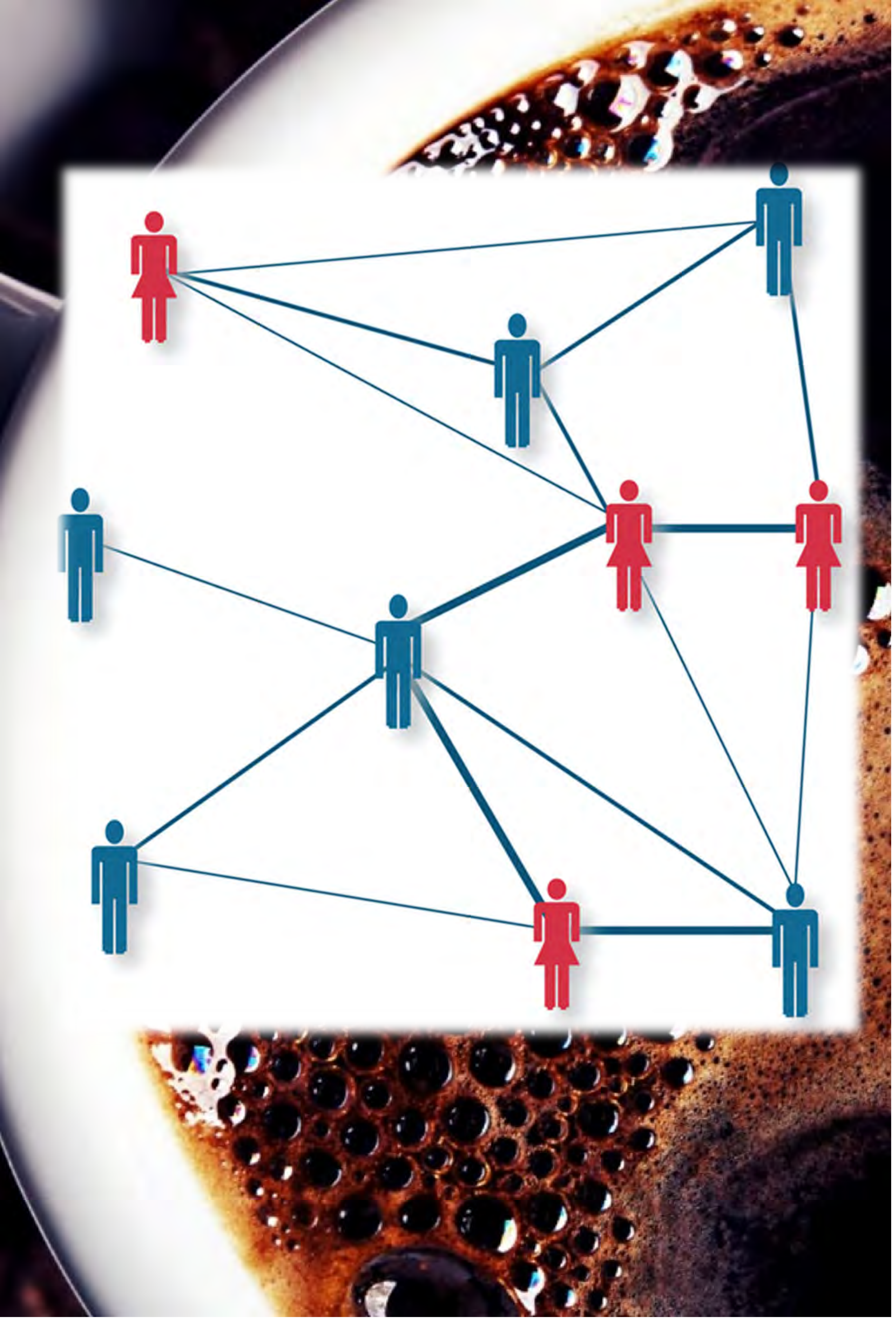
2. I really feel as if this organization's problems are my own. ____________

3. I do not feel like "part of the family" at my organization. ____________

4. I do not feel "emotionally attached" to this organization. ____________

5. This organization has a great deal of personal meaning for me. ____________

6. I do not feel a strong sense of belonging to my organization. ____________



Affective Commitment in response to a Social Network

- Affective commitment depends in large part on connections among people.

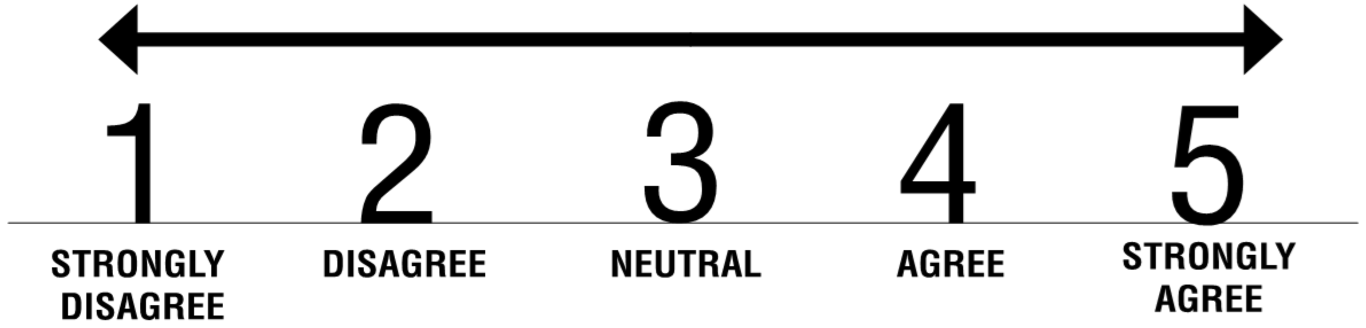
- Which person in this social network diagram is most at risk for turning over.

- The Erosion Model would say the individual with only one linkage to other people. This same sort of diagram is relevant to the Social Influence model, which argues that people with linkages to “leavers” will become at risk for turning over.

Continuance Commitment

- A desire on the part of an employee to remain a member of an organization because of an awareness of the costs associated with leaving it.
- You stay because you need to.
- What would you feel if you left anyway?
- You'd feel nervous or anxious. So continuance committed people stay, as much as anything, to avoid feeling anxiety

Continuance Commitment



1 STRONGLY DISAGREE

2 DISAGREE

3 NEUTRAL

4 AGREE

5 STRONGLY AGREE

1. **Quitting my job would bring with it major personal sacrifice.**
2. **I don’t have enough employment options to consider leaving right now.**
3. **It’s difficult to leave the organization because I don’t have anywhere else to go.**
4. **Staying in my current job is more a product of circumstances than preference.**
5. **Leaving my job now would bring significant personal disruption.**
6. **Frankly, I couldn’t quit my job now, even if it’s what I wanted to do.**

Embedded and Continuance Commitment

"Embedded" people feel:

FACET	FOR THE ORGANIZATION:	FOR THE COMMUNITY:
Links	• I've worked here for such a long time. • I'm serving on so many teams and committees.	• Several close friends and family live nearby. • My family's roots are in this community.
Fit	• My job utilizes my skills and talents well. • I like the authority and responsibility I have at this company.	• The weather where I live is suitable for me. • I think of the community where I live as home.
Sacrifice	• The retirement benefits provided by the organization are excellent. • I would sacrifice a lot if I left this job.	• People respect me a lot in my community. • Leaving this community would be very hard.

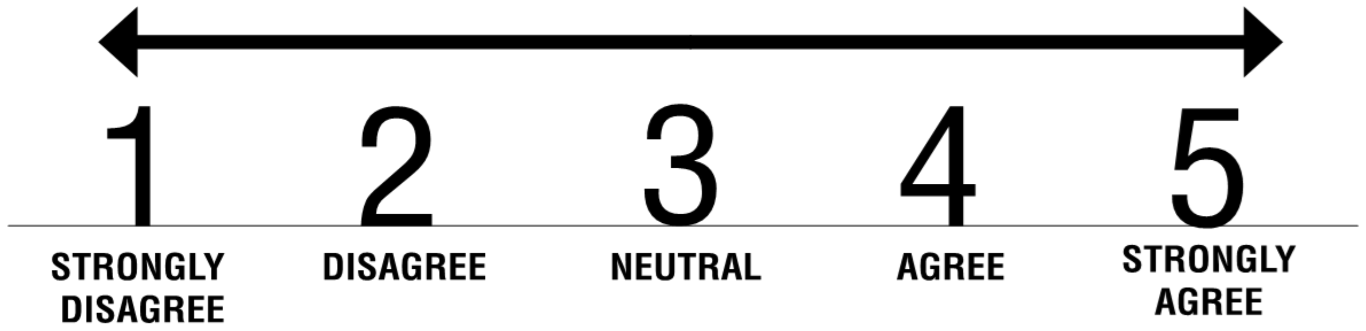
Normative Commitment

- A desire on the part of an employee to remain a member of an organization because of a feeling of obligation.

- You stay because you ought to.

- What would you feel if you left anyway?

Normative Commitment



1. **I have an obligation to stay with my company.**
2. I wouldn’t quit my job right now because I owe the company too much.
3. I owe this company for the things it’s given me.
4. Leaving my job now would fill me with significant guilt.
5. It just wouldn’t be right to think about quitting my job.
6. Staying with my organization is just something that I ought to do.

Organizational Commitment Exercise

- Consider the three scenarios depicted on the following slide.

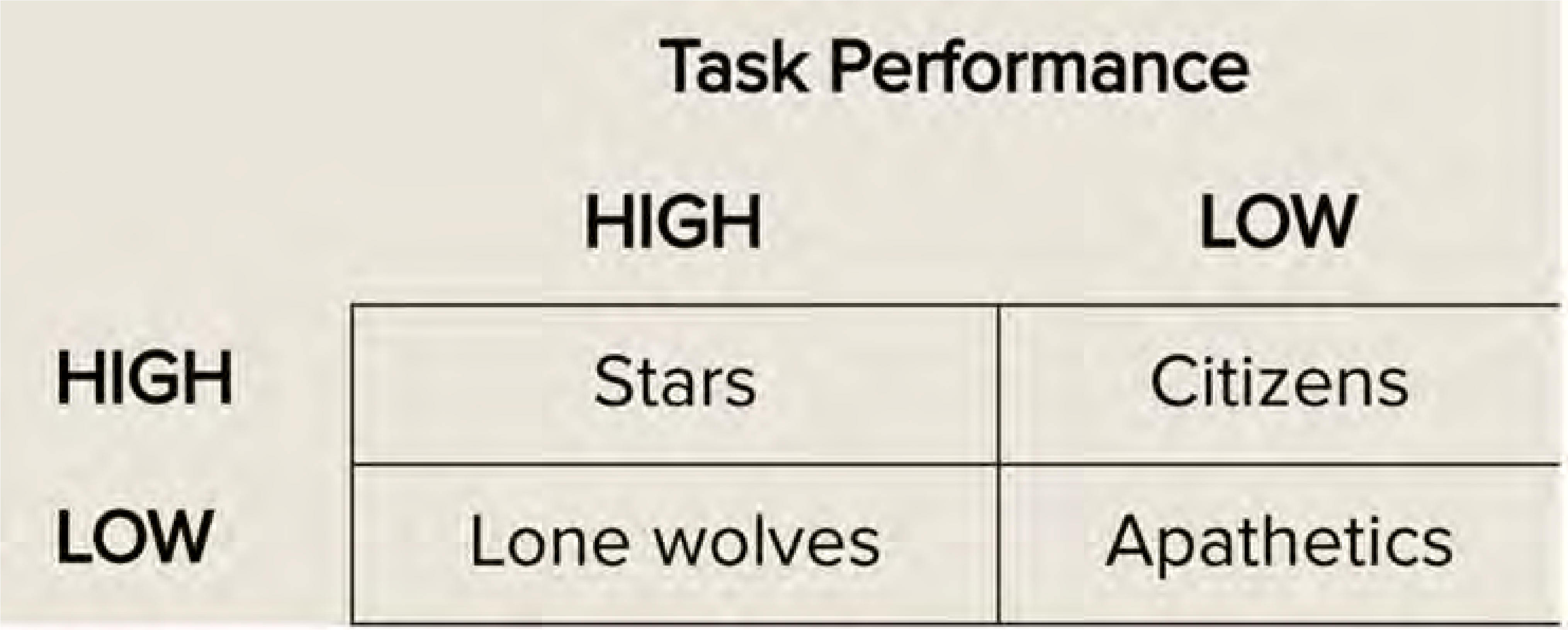
- Come to consensus on two specific behaviors that capture your likely response (that is, what you would probably do, as opposed to what you wish you would do).

Organizational Commitment Scenarios

Scenario	Description	Likely behaviors
Annoying Boss	You've been working at your current company for about a year. Over time, your boss has become more and more annoying to you. It's not that your boss is a bad person, or even necessarily a bad boss. It's more a personality conflict–the way your boss talks, the way your boss manages every little thing, even the facial expressions your boss uses. The more time passes, the more you just can't stand to be around your boss.	Two likely behaviors:
Boring Job	You've been working at your current company for about a year. You've come to realize that your job is pretty boring. It's the first real job you've ever had, and at first, it was nice to have some money and something to do every day. But the "new job" excitement has worn off, and things are actually quite monotonous. Same thing every day. It's to the point that you check your watch every hour, and Wednesdays feel like they should be Fridays.	Two likely behaviors:
Pay and Seniority	You've been working at your current company for about a year. The consensus is that you're doing a great job—you've gotten excellent performance evaluations and have emerged as a leader on many projects. As you've achieved this high status, however, you've come to feel that you're underpaid. Your company's pay procedures emphasize seniority much more than job performance. As a result, you look at other members of your project teams and see poor performers making much more than you, just because they've been with the company longer.	Two likely behaviors:

Four Types of Employees

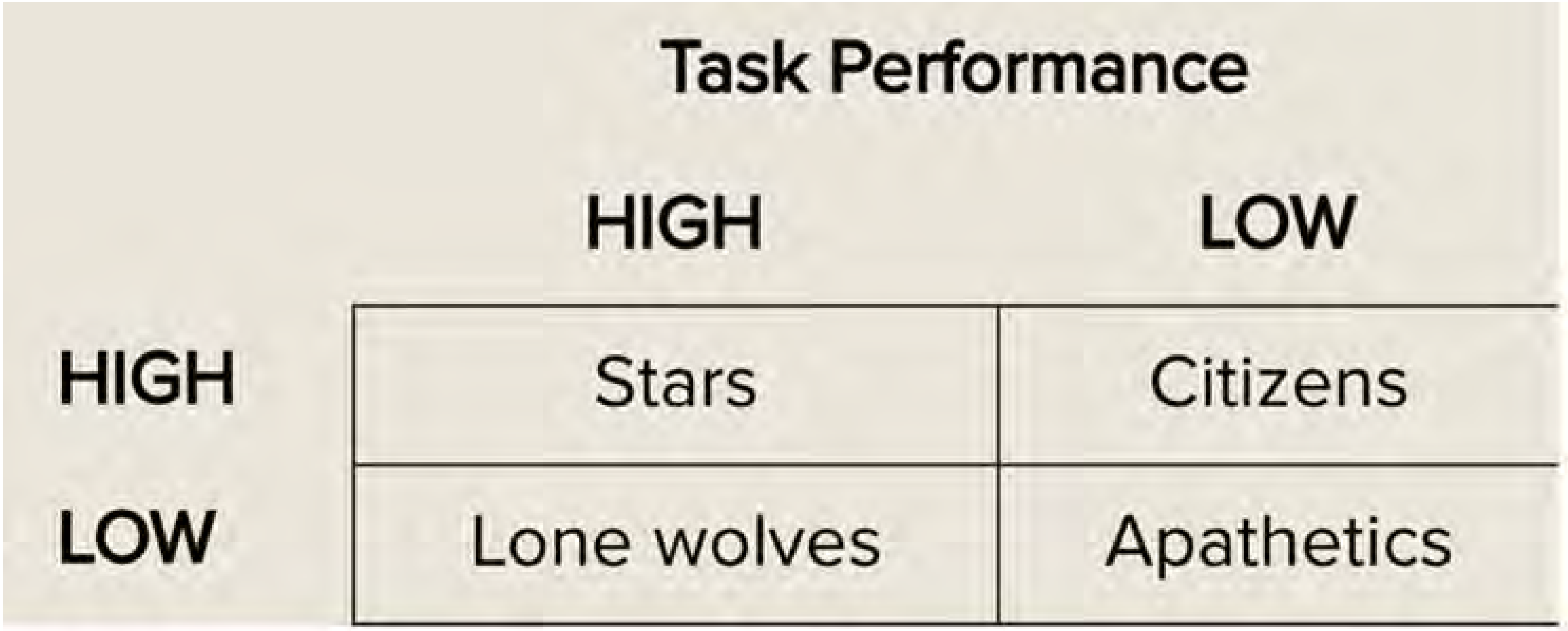
Which kind of employee do you think will engage in Exit, Voice, Loyalty, or Neglect?



	Task Performance	
	HIGH	LOW
HIGH	Stars	Citizens
LOW	Lone wolves	Apathetics

Four Types of Employees

The Star will engage in Voice, because they are motivated to improve the place and have the credibility to do so. The Lone Wolf also has the credibility, but not the motivation to improve, so they would engage in Exit. The Citizen will engage in Loyalty, and the Apathetic will engage in Neglect.

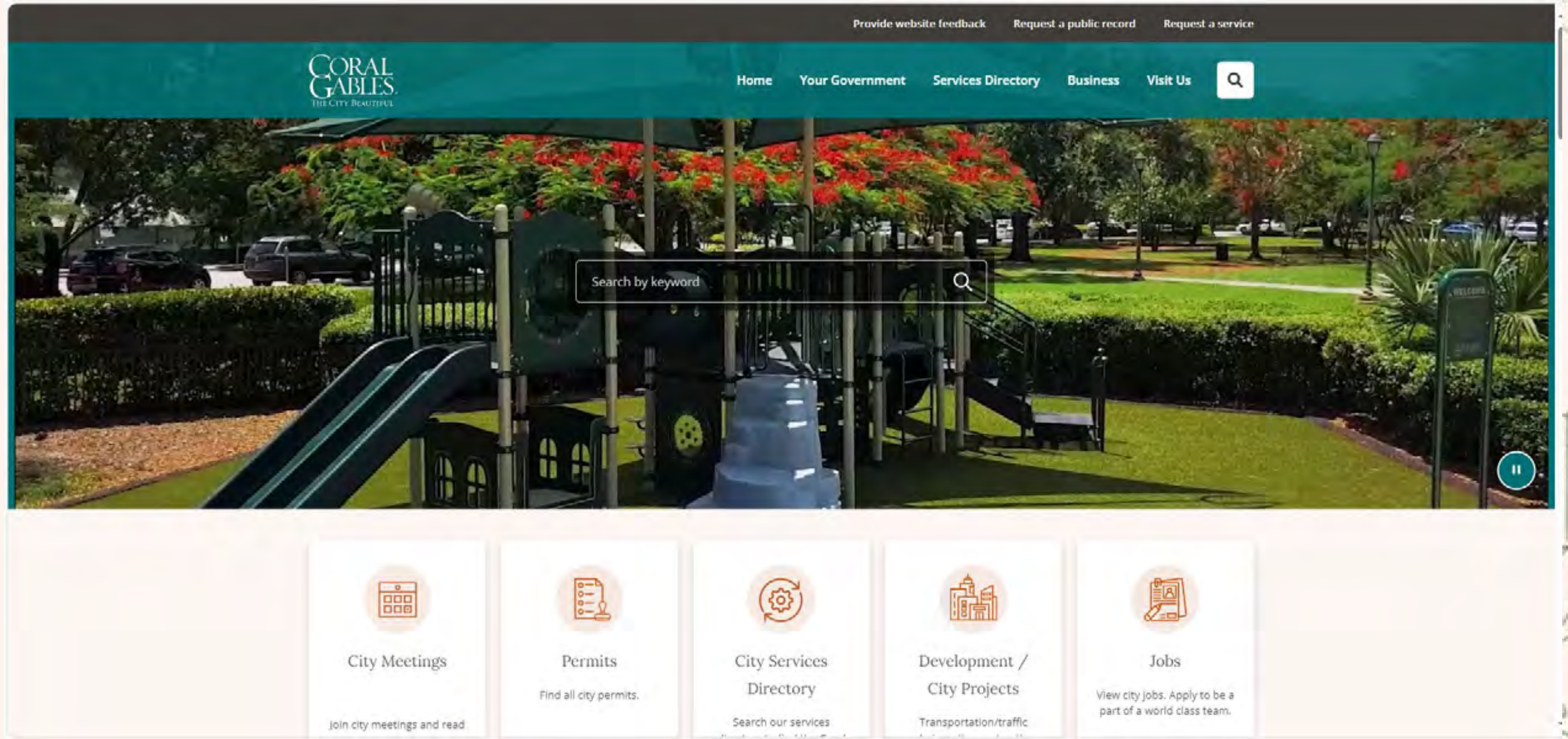


	Task Performance	
	HIGH	LOW
HIGH	Stars	Citizens
LOW	Lone wolves	Apathetics

Policies & Procedures

Policies & Procedures

- Do we have them?
- What are they?
- Where can you find them?
  - City webpage: www.coralgables.com
  - Intranet: City of Coral Gables Personnel Rules & Regulations – Human Resources
  - Department Policies & Handbooks: Parks Drive



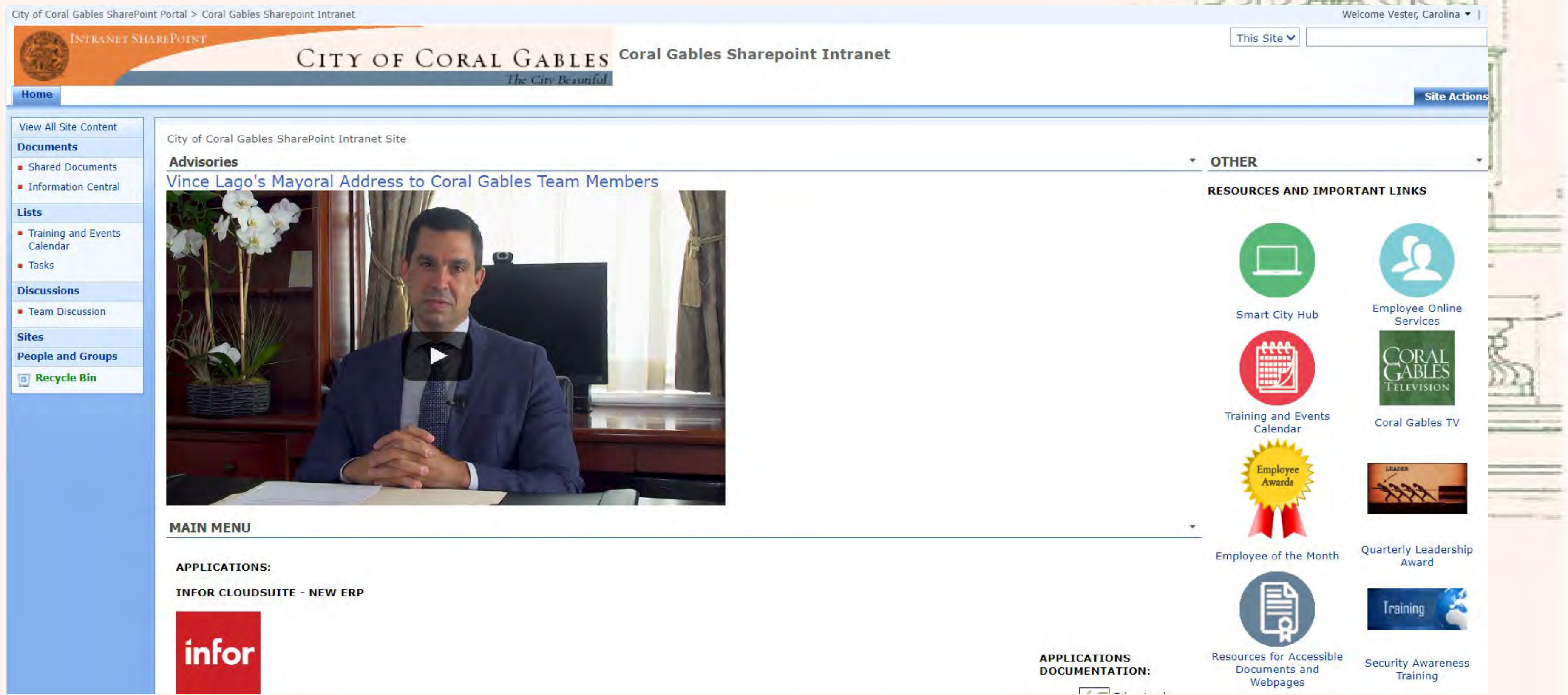
Join city meetings and read

Find all city permits.

Search our services

Transportation/traffic

View city jobs. Apply to be a part of a world class team.



City of Coral Gables SharePoint Intranet Site

Advisories

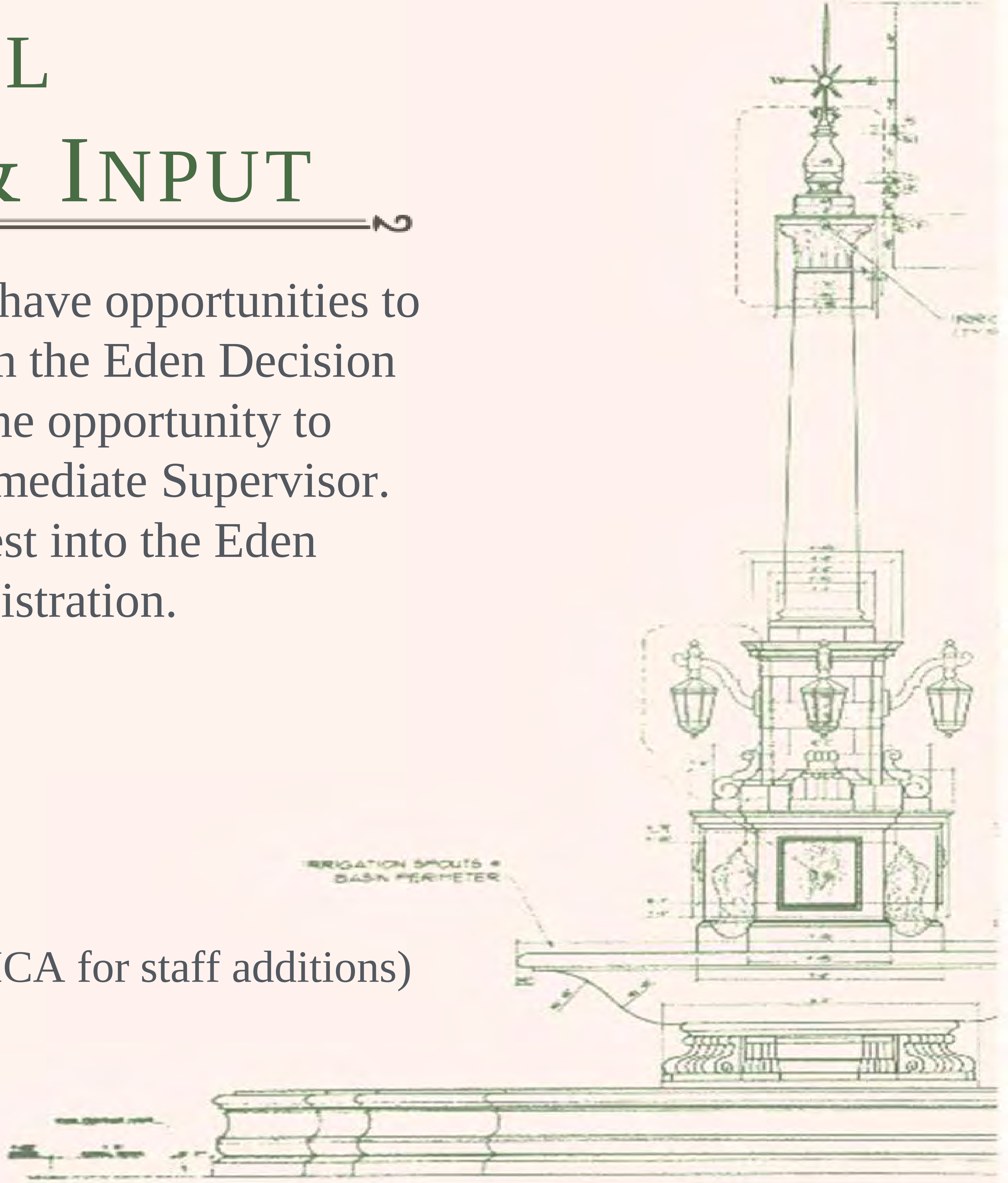
Vince Lago's Mayoral Address to Coral Gables Team Members

Personnel Involvement & Input

- Administration will provide opportunities for staff to provide input on all matters pertaining to Parks and Community Recreation Operations. These opportunities will occur at a minimum in these instances:
  - Annual Meeting
  - Annual Leadership Retreat
  - Leadership Workshops
  - Monthly Supervisor Meetings
  - Division Specific Monthly Part-Time In-Service Trainings
  - One-On-One Meetings
  - On-going Development Conversations

Personnel Involvement & Input

- **Budget Recommendations:** Staff will have opportunities to submit budget recommendations through the Eden Decision Package process. Each staff will have the opportunity to provide new budget requests to their immediate Supervisor. The Supervisor will then input the request into the Eden system with the assistance of the Administration.
- Each request must include:
  - The justification for the request
  - The amount of funding needed
  - Anticipated revenue
  - Related costs (including benefits, FICA for staff additions)
  - Duration of needed funds



Master Plans
& Future Planning

Community Recreation And War Memorial Youth Center Master Plan Updates

City of Coral Gables
Community Recreation

Coral Gables
The City Beautiful

Community Recreation Master Plan
Quick Review

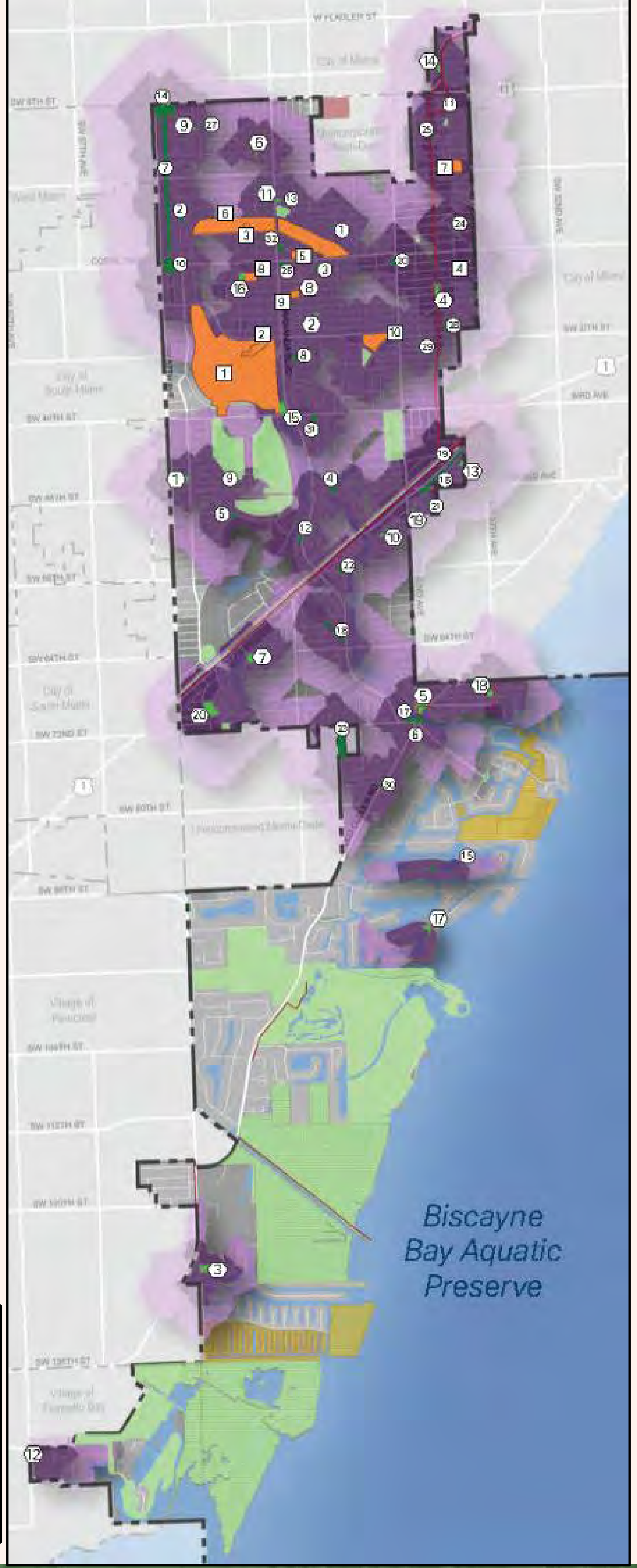
- The Community Recreation Master Plan and the War Memorial Youth Center Master Plan were adopted by the City Commission on September 28, 2021. coralgables.com/communityrecreationmasterplan
- The purpose of the plan is to provide staff with a roadmap of project priorities for its facilities, parks and open spaces for the next 10 – 15 years.
- A sunshine meeting was held on Thursday, Feb. 24, 2022, to discuss the phasing and funding of the plan using a referendum option through general obligation bonds.
- Currently funding is contingent upon CIP budget funds and impact fees until future discussion can be held to discuss additional funding opportunities.

2021 Coral Gables

Community Recreation Master Plan

Community Recreation Master Plan
Level of Service

- Acreage: 5.24 Acres /1,000 residents.
  - 260 acres of City-managed parks, 49,700 residents.
- Facilities: Coral Gables has a surplus of basketball courts, tennis courts, and soccer fields when compared to SCORP LOS figures.
- Access to neighborhood parks is experiencing gaps in the southern part of the City but is balanced by larger preserves and greenspace not available in the northern, more urban areas.
  - Every home should be within a 10-minute walk of a meaningful open space.



▨ 10-minute walk

▨ 20-minute walk

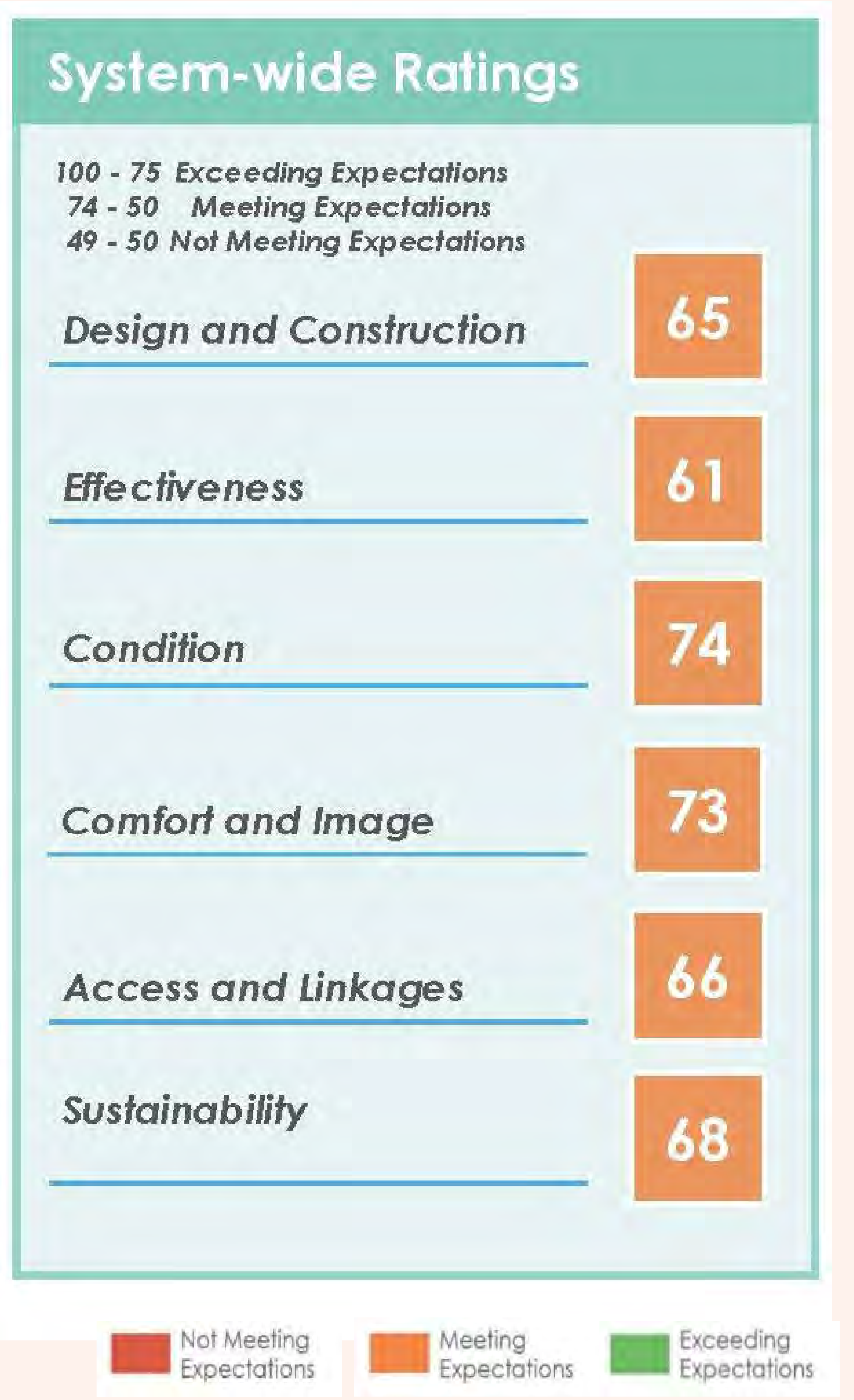
Community Recreation Master Plan
Existing Ratings

SUCCESSES

- High level of maintenance.
- Most sites clean and free of litter, with a feeling of perceived safety.
- Parks make a good impression.
- Most parks and facilities provide a high level of comfort.

OPPORTUNITIES

- Enhance neighborhood access.
- Wayfinding and signage standards.
- Consistent application of design standards.
- Improvement in environmental sustainability, awareness, and education.
- Light touches and refreshments for functionality and comfort.
- ***Many improvements currently completed or underway!***



System-wide Ratings

100 - 75 Exceeding Expectations
74 - 50 Meeting Expectations
49 - 50 Not Meeting Expectations

Design and Construction	65
Effectiveness	61
Condition	74
Comfort and Image	73
Access and Linkages	66
Sustainability	68

🟥 Not Meeting Expectations 🟧 Meeting Expectations 🟩 Exceeding Expectations

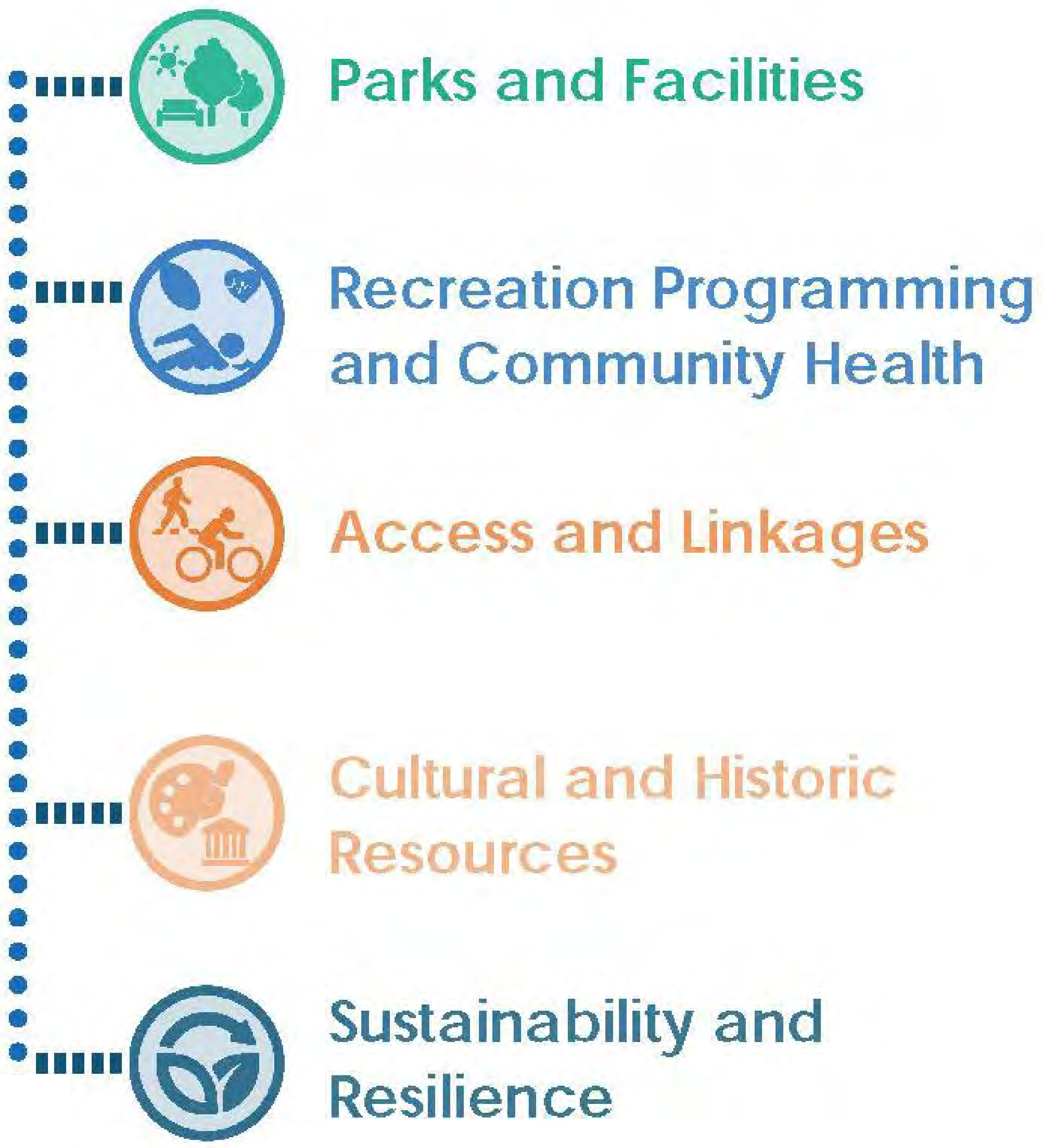
Community Recreation Master Plan
Needs & Priorities Summary

- Maintain and enhance existing parks and facilities.
- Improve safety and security in parks and nearby areas.
- Provide new walking and biking trails.
- Improve communication between the parks and recreation department and the community.
- Promote equitable access to parks through enhanced connectivity and walkability.
- **WMYC**
  - Expand athletics and program offerings.
  - Increase participation capacity.
  - Improve access to the center.

Community Recreation Master Plan
Vision Subsystems

- The Vision for the CRMP is build around a set of five subsystems that were established to help guide the development of the parks and facilities across the system.

- The guiding principles and vision recommendations for each of these subsystems are intended to guide the parks and recreation system over the next 10 years.


Parks and Facilities

Recreation Programming and Community Health

Access and Linkages

Cultural and Historic Resources

Sustainability and Resilience

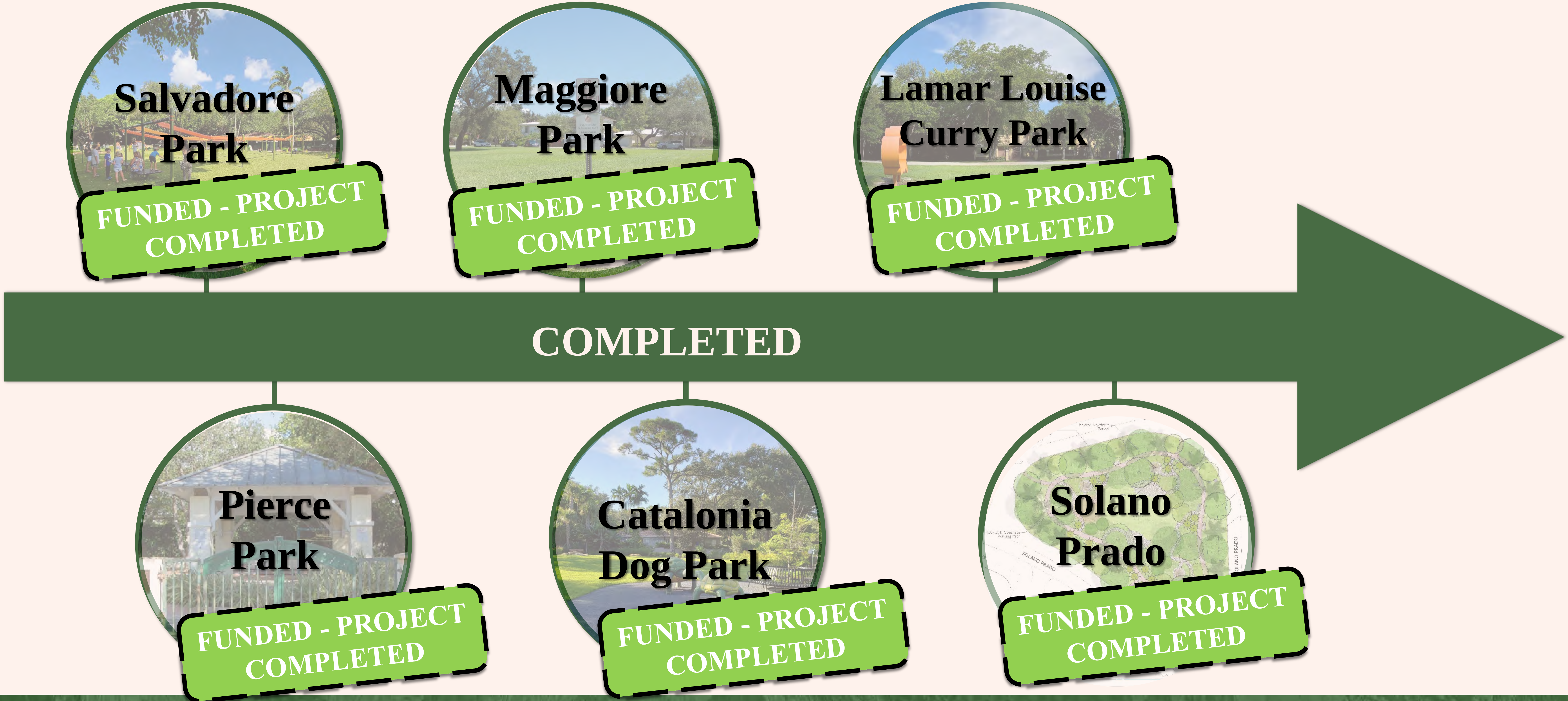
Community Recreation Master Plan
Funding And Phasing – why?

- While parks and recreational activities have always been viewed as “quality of life”, current conditions have brought forth the importance of parks and facilities as a vital component for health and well-being.
- Whether it is for physical health from exercise and athletics or mental health benefits from nature and socialization, our parks and facilities are now more vital than ever.

Community Recreation Master Plan
Funding And Phasing – Future Funding Options?

- The completion of the master plan will require approximately $160 million through different funding phases.
- The required funds are not available within the current City budget.
- A bond would provide a mechanism to attain these funds over the implementation period of the master plan.

Community Recreation Master Plan – **Completed**



Salvadore Park

FUNDED - PROJECT COMPLETED

Maggiore Park

FUNDED - PROJECT COMPLETED

Lamar Louise Curry Park

FUNDED - PROJECT COMPLETED

COMPLETED

Pierce Park

FUNDED - PROJECT COMPLETED

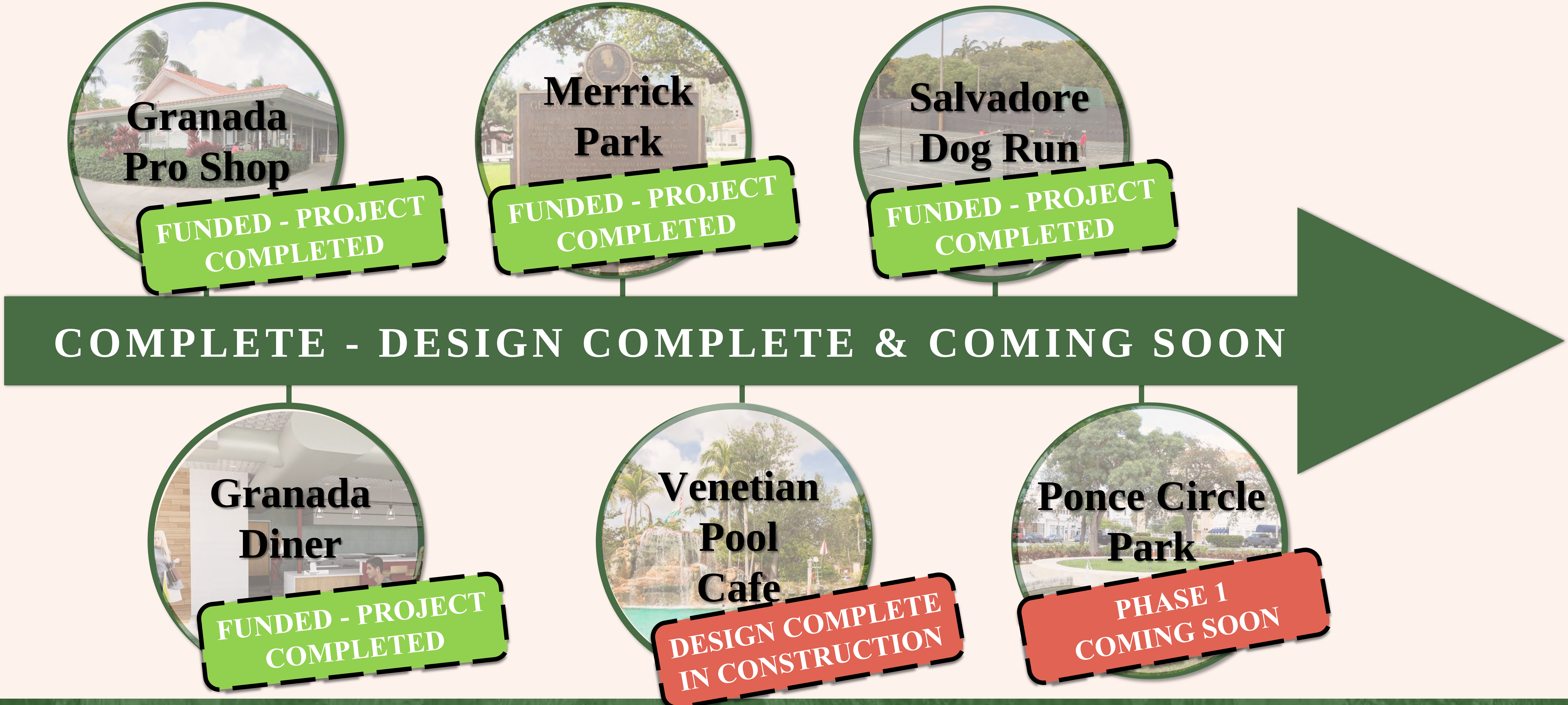
Catalonia Dog Park

FUNDED - PROJECT COMPLETED

Solano Prado

FUNDED - PROJECT COMPLETED

Community Recreation Master Plan



COMPLETE - DESIGN COMPLETE & COMING SOON

Granada Pro Shop
FUNDED - PROJECT COMPLETED

Merrick Park
FUNDED - PROJECT COMPLETED

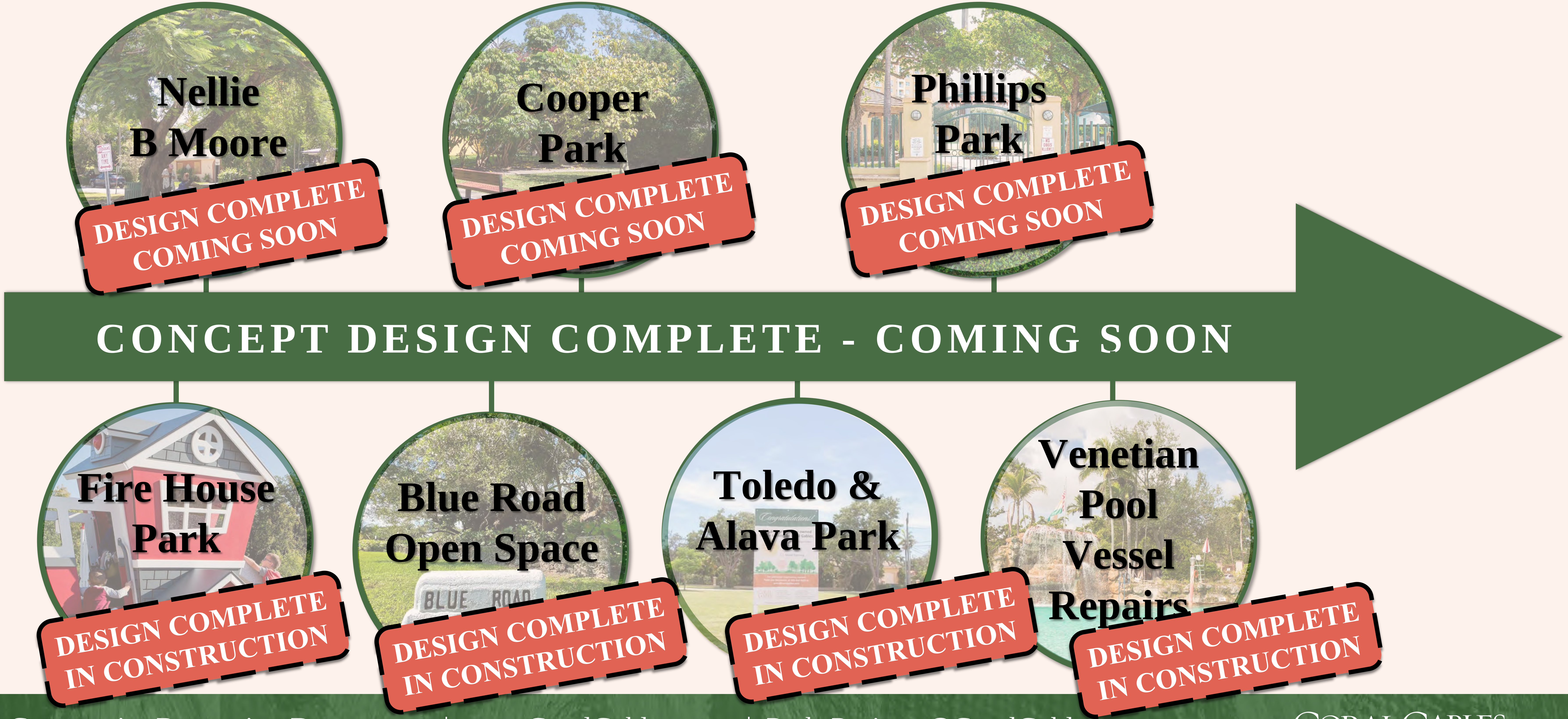
Salvadore Dog Run
FUNDED - PROJECT COMPLETED

Granada Diner
FUNDED - PROJECT COMPLETED

Venetian Pool Cafe
DESIGN COMPLETE IN CONSTRUCTION

Ponce Circle Park
PHASE 1 COMING SOON

Community Recreation Master Plan



Nellie B Moore

DESIGN COMPLETE COMING SOON

Cooper Park

DESIGN COMPLETE COMING SOON

Phillips Park

DESIGN COMPLETE COMING SOON

CONCEPT DESIGN COMPLETE - COMING SOON

Fire House Park

DESIGN COMPLETE IN CONSTRUCTION

Blue Road Open Space

DESIGN COMPLETE IN CONSTRUCTION

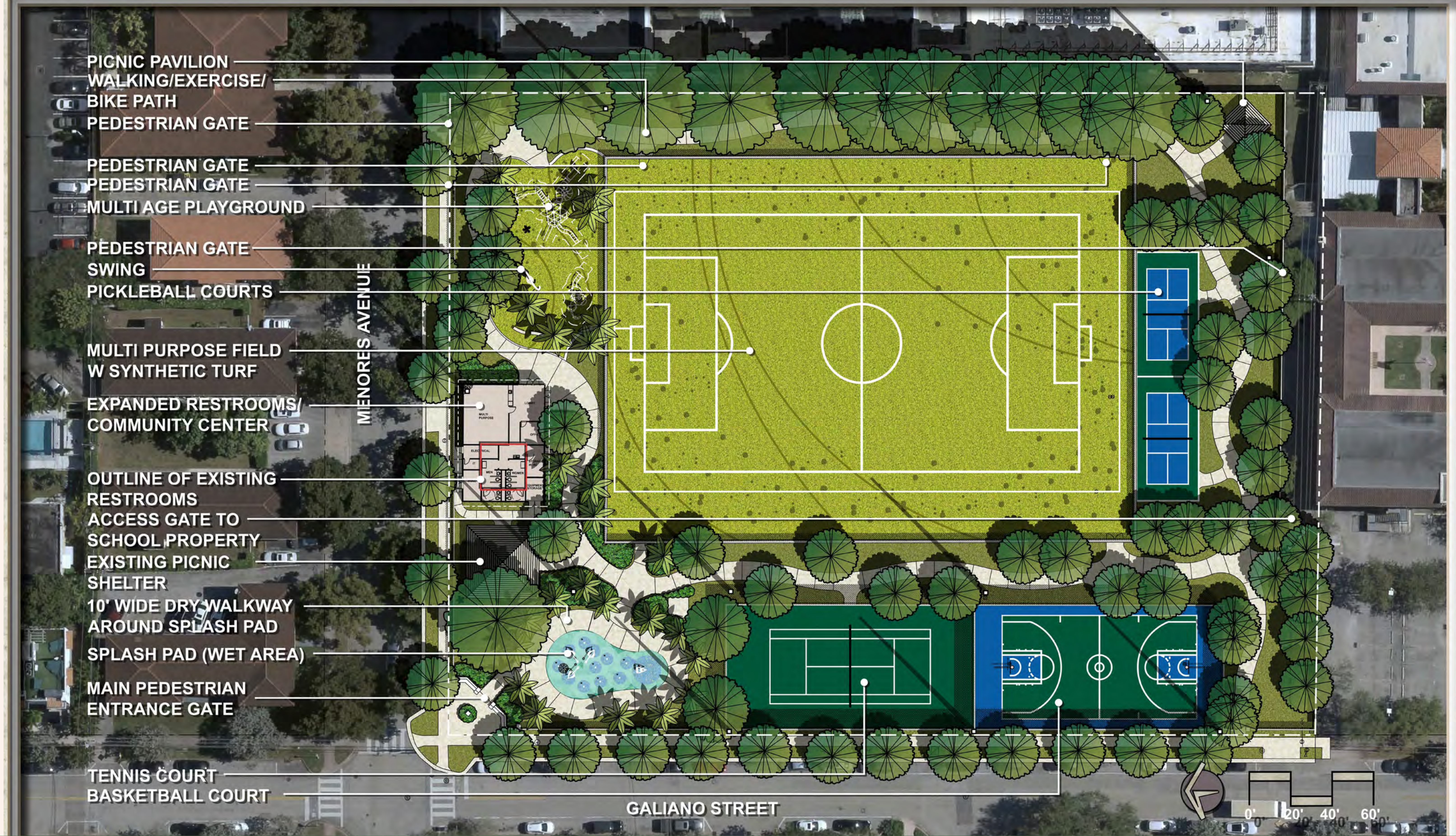
Toledo & Alava Park

DESIGN COMPLETE IN CONSTRUCTION

Venetian Pool Vessel Repairs

DESIGN COMPLETE IN CONSTRUCTION

Phillips Park Concept



PICNIC PAVILION

WALKING/EXERCISE/ BIKE PATH

PEDESTRIAN GATE

PEDESTRIAN GATE

PEDESTRIAN GATE

MULTI AGE PLAYGROUND

PEDESTRIAN GATE

SWING

PICKLEBALL COURTS

MULTI PURPOSE FIELD W SYNTHETIC TURF

EXPANDED RESTROOMS/ COMMUNITY CENTER

OUTLINE OF EXISTING RESTROOMS

ACCESS GATE TO SCHOOL PROPERTY

EXISTING PICNIC SHELTER

10' WIDE DRY WALKWAY AROUND SPLASH PAD

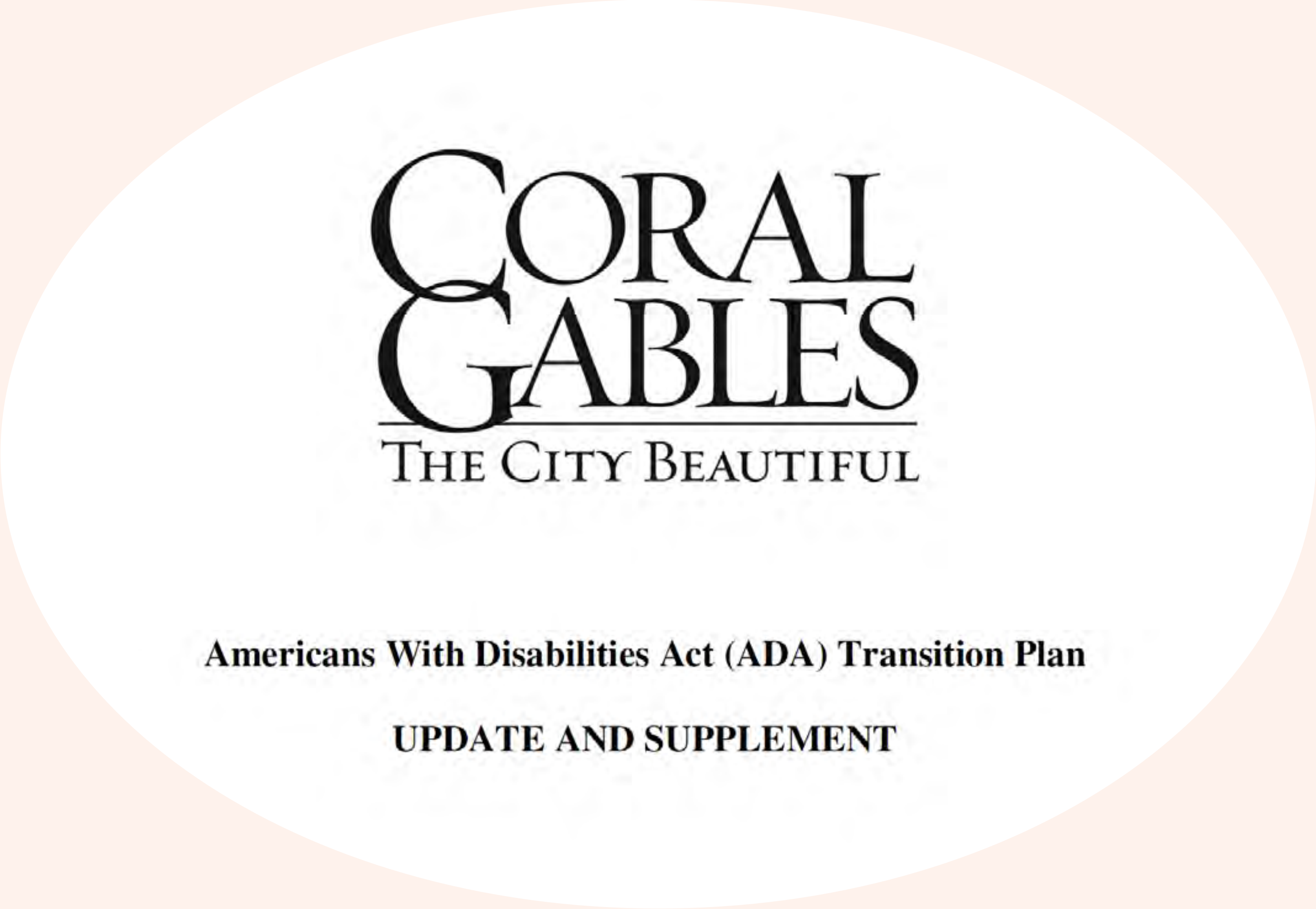
SPLASH PAD (WET AREA)

MAIN PEDESTRIAN ENTRANCE GATE

TENNIS COURT

BASKETBALL COURT

ADA Transition Plan Updates

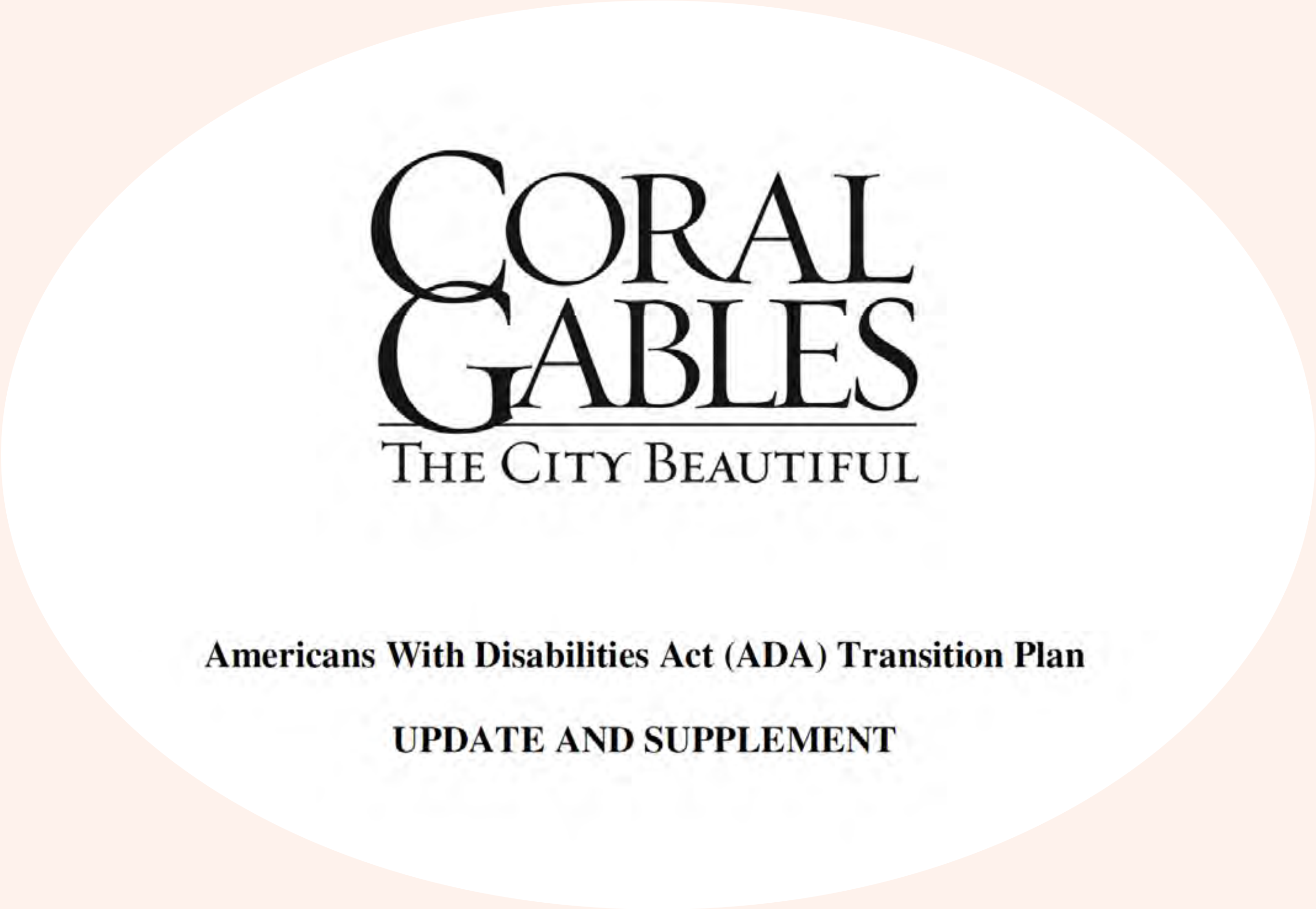


CORAL GABLES
THE CITY BEAUTIFUL

Americans With Disabilities Act (ADA) Transition Plan

UPDATE AND SUPPLEMENT

The City of Coral Gables, Florida (the “City”) welcomes individuals with disabilities (residents and visitors). The City is committed to complying with Title II of the Americans With Disabilities Act (“ADA”) and related laws, and to fostering the principles of inclusion for individuals with disabilities in all aspects of the City’s activities, programs and services and beyond.



CORAL GABLES

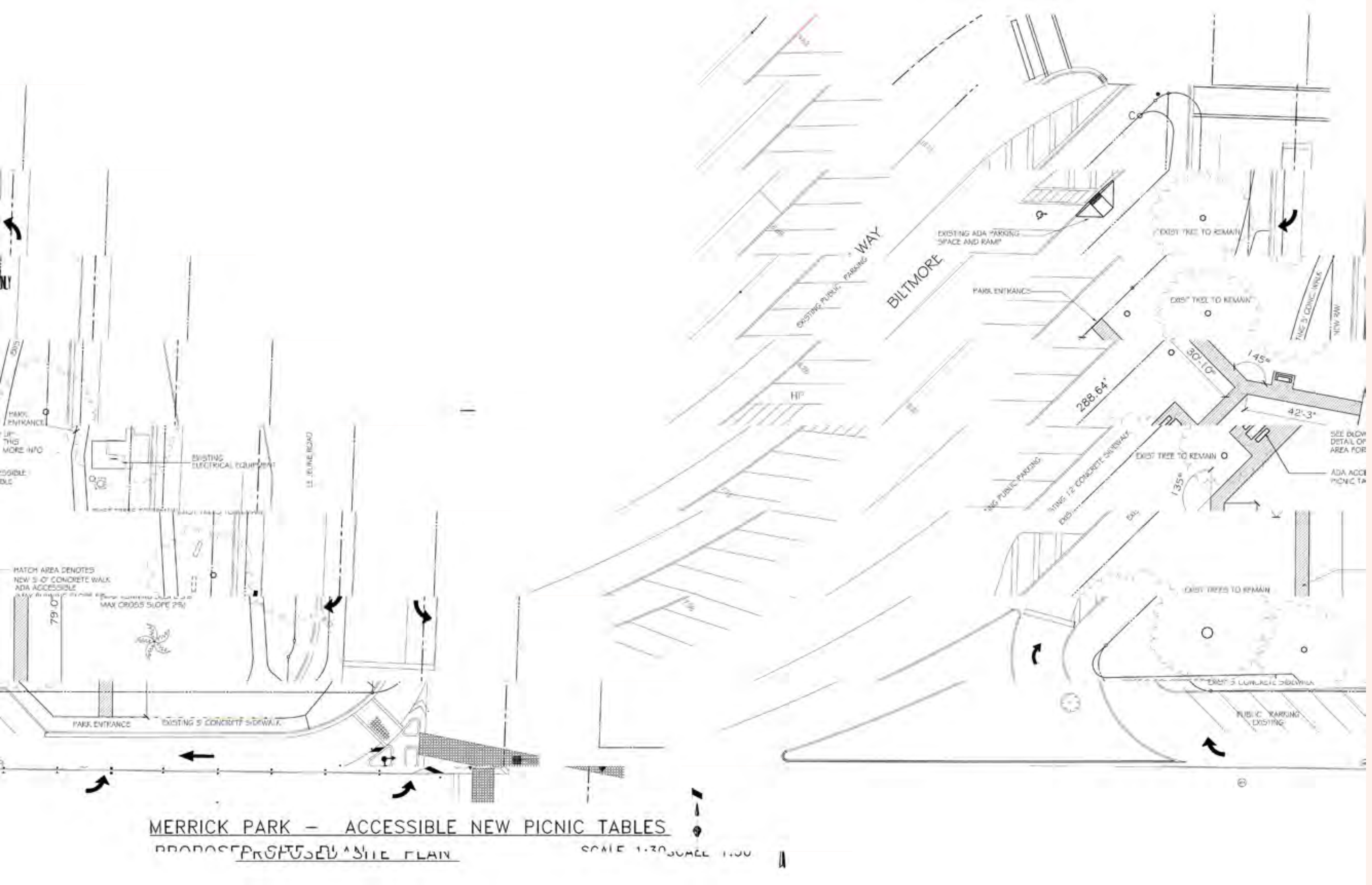
THE CITY BEAUTIFUL

Americans With Disabilities Act (ADA) Transition Plan

UPDATE AND SUPPLEMENT

The City’s Transition Plan is developed in accordance with Title II of the ADA, Chapter 11 of the Florida Building Code (“Florida Accessibility Code”) and related laws. The City has evaluated its physical facilities and their adjacent public rights-of-way to identify the modifications necessary to meet the applicable accessibility requirements

ADA Transition Plan Updates

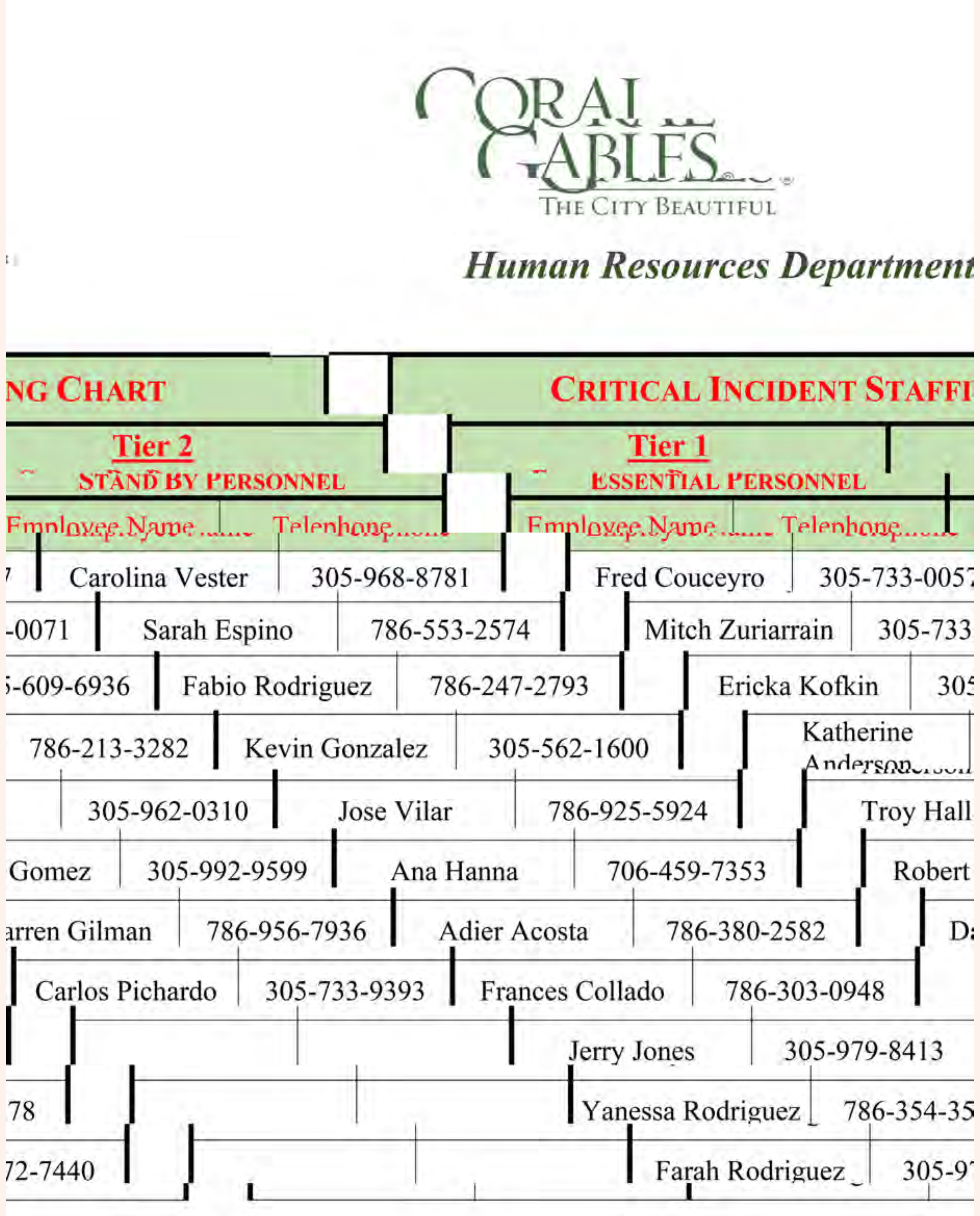


ADA Department Improvement Projects:

- Merrick Park ADA Walkway and furnishings.
- Coral Gables Golf & Country Club ADA site audit and respective improvements.
- Pierce Park renovation included ADA entrances, walkways and furnishings.

Records Disaster Mitigation and Recovery Plan Update

Records Disaster Mitigation and Recovery Plan



CORAL GABLES
THE CITY BEAUTIFUL

Human Resources Department

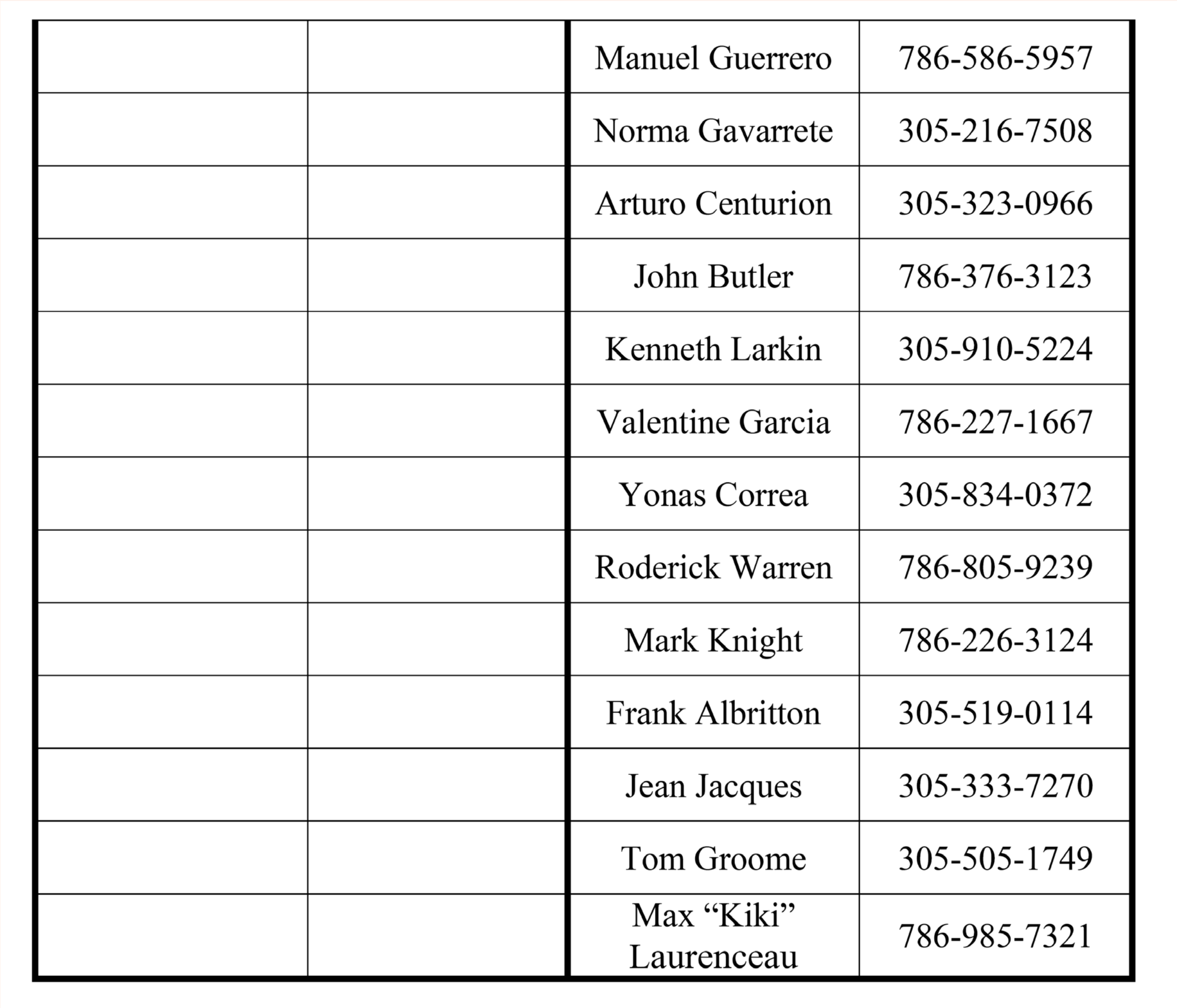
NG CHART | CRITICAL INCIDENT STAFFI

Tier 2 STAND BY PERSONNEL | Tier 1 ESSENTIAL PERSONNEL

Employee Name | Telephone | Employee Name | Telephone

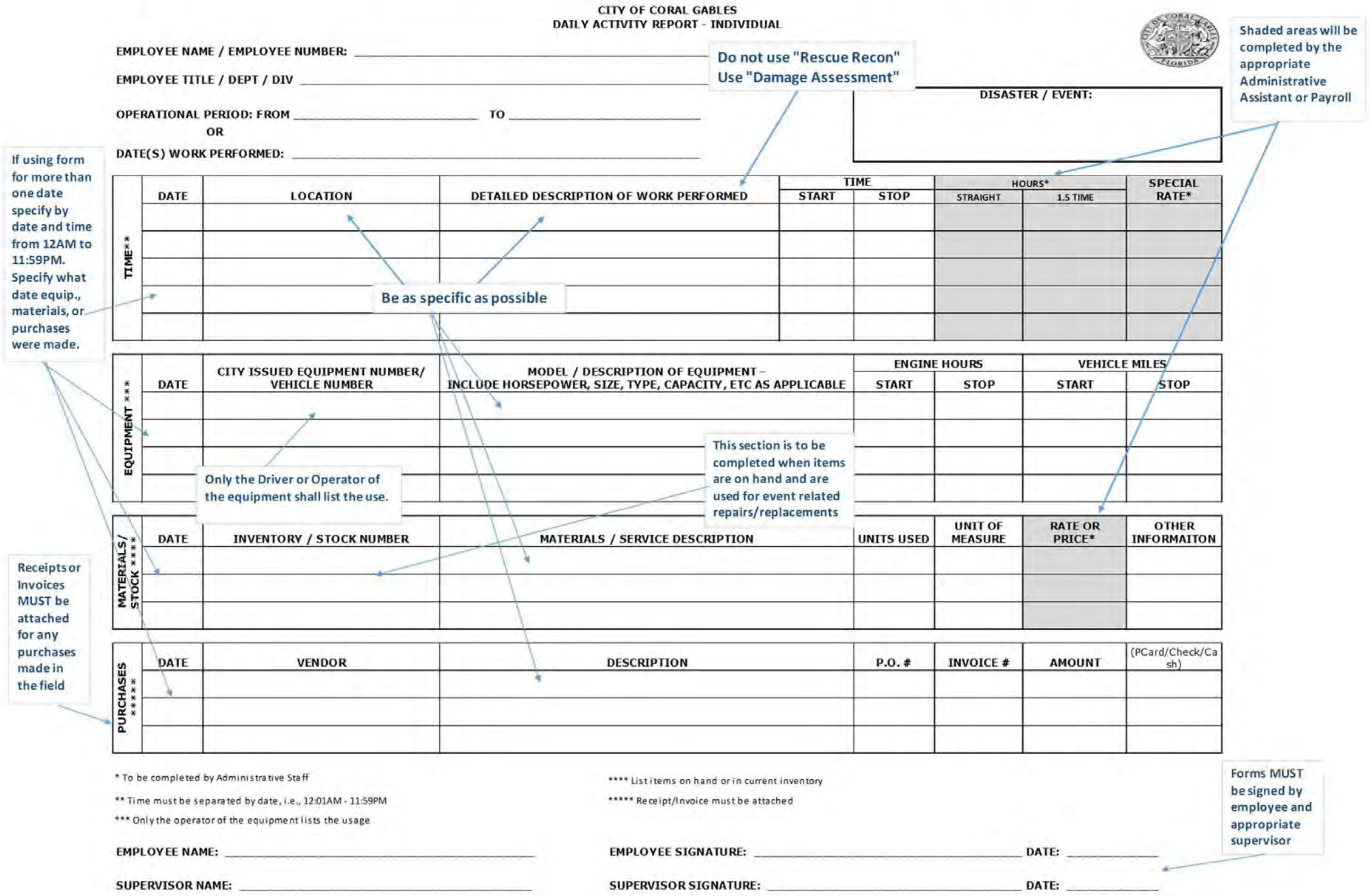
Carolina Vester 305-968-8781 Fred Couceyro 305-733-0057
-0071 Sarah Espino 786-553-2574 Mitch Zuriarrain 305-733
-609-6936 Fabio Rodriguez 786-247-2793 Ericka Kofkin 305
786-213-3282 Kevin Gonzalez 305-562-1600 Katherine Anderson
305-962-0310 Jose Vilar 786-925-5924 Troy Hall
Gomez 305-992-9599 Ana Hanna 706-459-7353 Robert
arren Gilman 786-956-7936 Adier Acosta 786-380-2582 Da
Carlos Pichardo 305-733-9393 Frances Collado 786-303-0948
Jerry Jones 305-979-8413
78 Yanessa Rodriguez 786-354-35
72-7440 Farah Rodriguez 305-9

- Emergency Management Hurricane Plan:
  - Update Critical Incident Staffing Chart



		Manuel Guerrero	786-586-5957
		Norma Gavarrete	305-216-7508
		Arturo Centurion	305-323-0966
		John Butler	786-376-3123
		Kenneth Larkin	305-910-5224
		Valentine Garcia	786-227-1667
		Yonas Correa	305-834-0372
		Roderick Warren	786-805-9239
		Mark Knight	786-226-3124
		Frank Albritton	305-519-0114
		Jean Jacques	305-333-7270
		Tom Groome	305-505-1749
		Max “Kiki” Laurenceau	786-985-7321

Individual Daily Activity Report



CITY OF CORAL GABLES
DAILY ACTIVITY REPORT - INDIVIDUAL

EMPLOYEE NAME / EMPLOYEE NUMBER: ______________________

EMPLOYEE TITLE / DEPT / DIV ______________________

OPERATIONAL PERIOD: FROM ______________ TO ______________
OR
DATE(S) WORK PERFORMED: ______________________

DISASTER / EVENT:

Do not use "Rescue Recon"
Use "Damage Assessment"

Shaded areas will be completed by the appropriate Administrative Assistant or Payroll

If using form for more than one date specify by date and time from 12AM to 11:59PM. Specify what date equip., materials, or purchases were made.

				TIME		HOURS*		SPECIAL RATE*
TIME**	DATE	LOCATION	DETAILED DESCRIPTION OF WORK PERFORMED	START	STOP	STRAIGHT	1.5 TIME	

Be as specific as possible

				ENGINE HOURS		VEHICLE MILES	
EQUIPMENT ***	DATE	CITY ISSUED EQUIPMENT NUMBER/ VEHICLE NUMBER	MODEL / DESCRIPTION OF EQUIPMENT – INCLUDE HORSEPOWER, SIZE, TYPE, CAPACITY, ETC AS APPLICABLE	START	STOP	START	STOP

Only the Driver or Operator of the equipment shall list the use.

This section is to be completed when items are on hand and are used for event related repairs/replacements

MATERIALS / STOCK ****	DATE	INVENTORY / STOCK NUMBER	MATERIALS / SERVICE DESCRIPTION	UNITS USED	UNIT OF MEASURE	RATE OR PRICE*	OTHER INFORMAITON

Receipts or Invoices MUST be attached for any purchases made in the field

PURCHASES *****	DATE	VENDOR	DESCRIPTION	P.O. #	INVOICE #	AMOUNT	(PCard/Check/Cash)

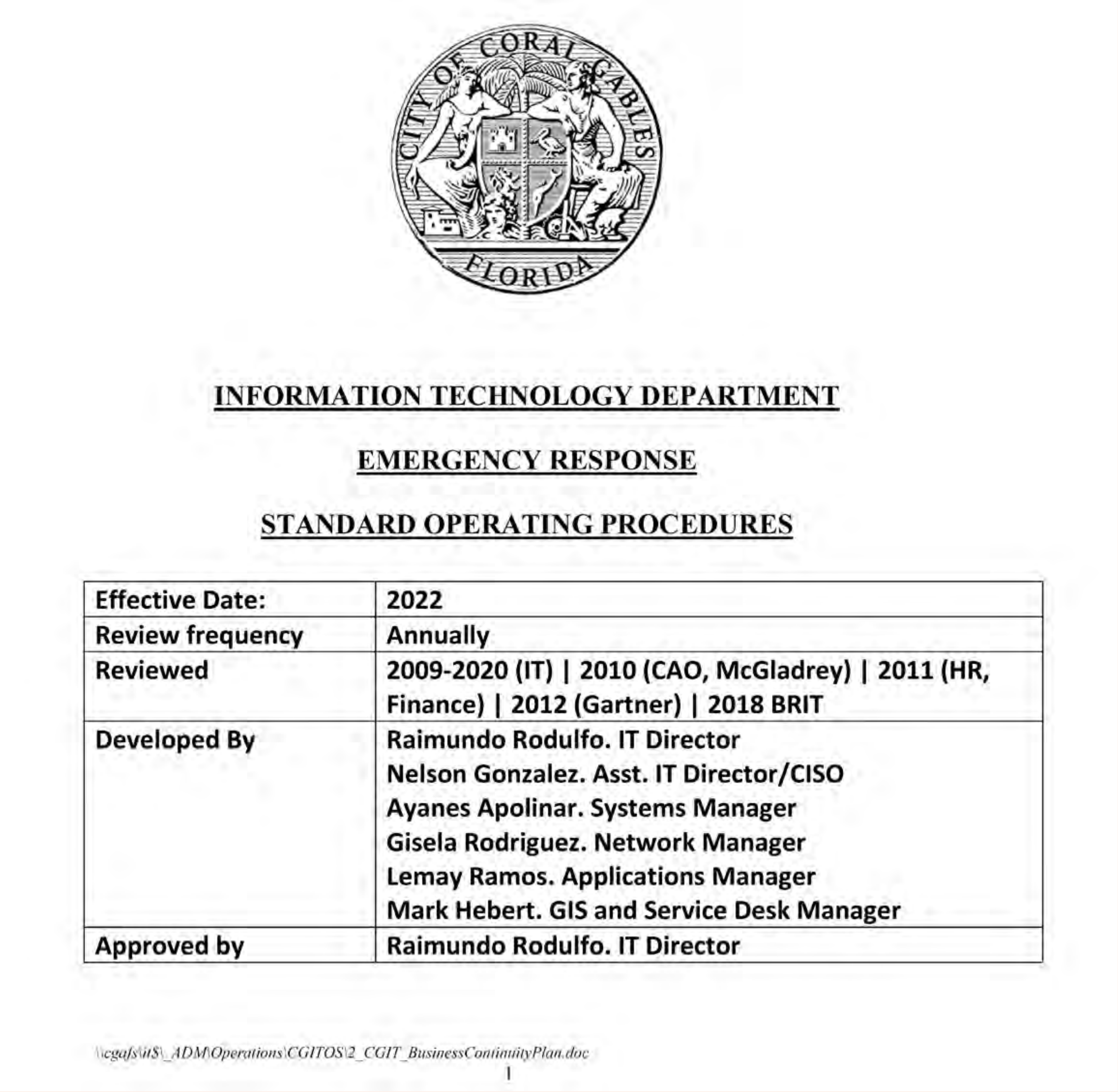
* To be completed by Administrative Staff
** Time must be separated by date, i.e., 12:01AM - 11:59PM
*** Only the operator of the equipment lists the usage
**** List items on hand or in current inventory
***** Receipt/Invoice must be attached

Forms MUST be signed by employee and appropriate supervisor

EMPLOYEE NAME: ______________ EMPLOYEE SIGNATURE: ______________ DATE: ________

SUPERVISOR NAME: ______________ SUPERVISOR SIGNATURE: ______________ DATE: ________

Records Disaster Mitigation and Recovery Plan



INFORMATION TECHNOLOGY DEPARTMENT

EMERGENCY RESPONSE

STANDARD OPERATING PROCEDURES

Effective Date:	2022
Review frequency	Annually
Reviewed	2009-2020 (IT) | 2010 (CAO, McGladrey) | 2011 (HR, Finance) | 2012 (Gartner) | 2018 BRIT
Developed By	Raimundo Rodulfo. IT Director Nelson Gonzalez. Asst. IT Director/CISO Ayanes Apolinar. Systems Manager Gisela Rodriguez. Network Manager Lemay Ramos. Applications Manager Mark Hebert. GIS and Service Desk Manager
Approved by	Raimundo Rodulfo. IT Director

\\cgafs\it$_ADM\Operations\CGITOS\2_CGIT_BusinessContinuityPlan.doc

1

- CGIT Business Continuity Plan:
  - Revised in 2022 by IT Department

Trivia Question #5

What two life altering events brought on the decline of George Merrick and the bankruptcy of Coral Gables?

Correct Answer to Question #5

THE GREAT DEPRESSION &

THE HURRICANE OF 1935

INFOR Employee Login

INTRANET - INFOR LIVE SITE

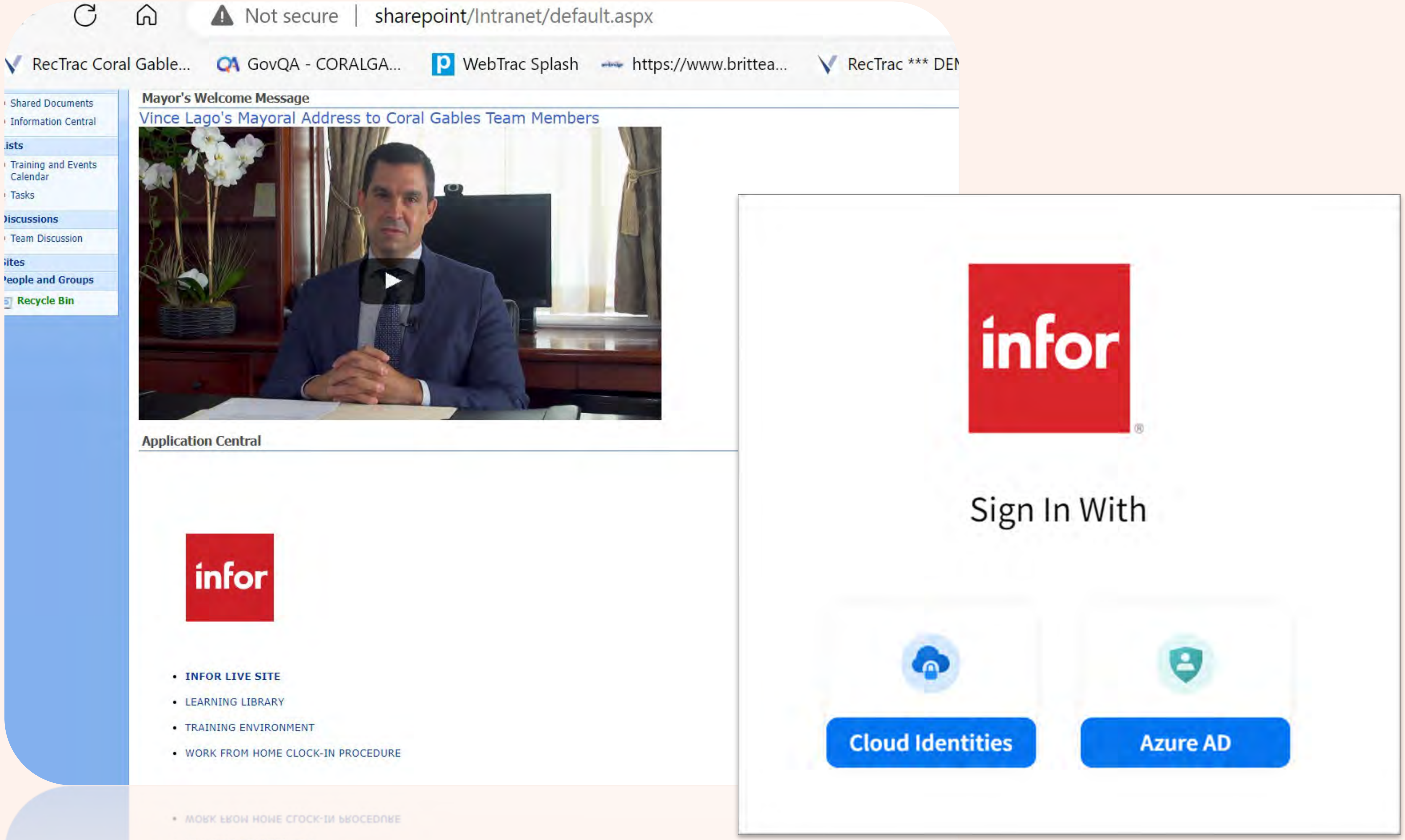
http://sharepoint/Intranet/default.aspx

Select

- Infor

Live Site

- Azure AD



Mayor's Welcome Message

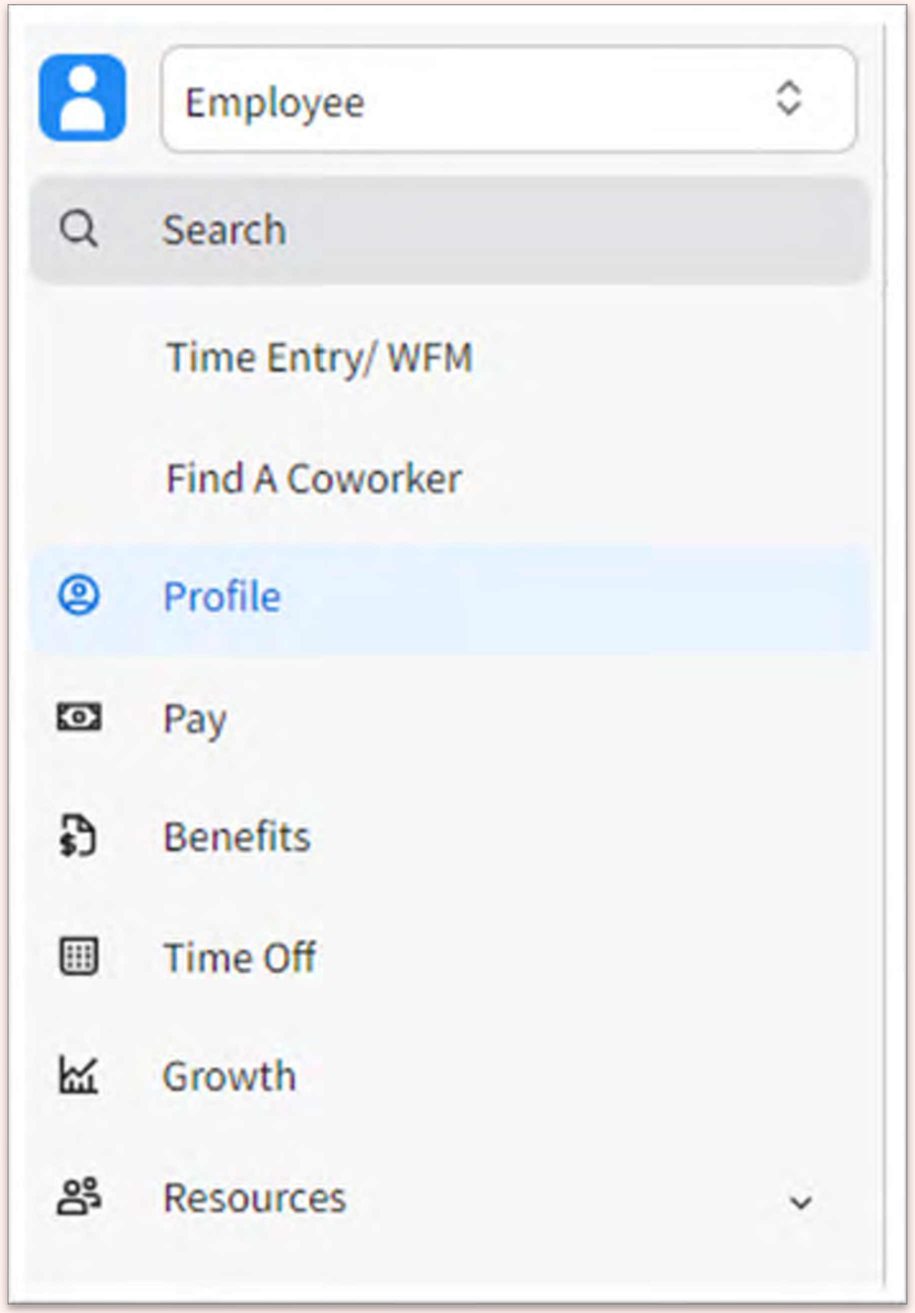
Vince Lago's Mayoral Address to Coral Gables Team Members

Application Central

- INFOR LIVE SITE
- LEARNING LIBRARY
- TRAINING ENVIRONMENT
- WORK FROM HOME CLOCK-IN PROCEDURE

Sign In With

Intranet - INFOR Live Site



Employee

Search

Time Entry/ WFM

Find A Coworker

Profile

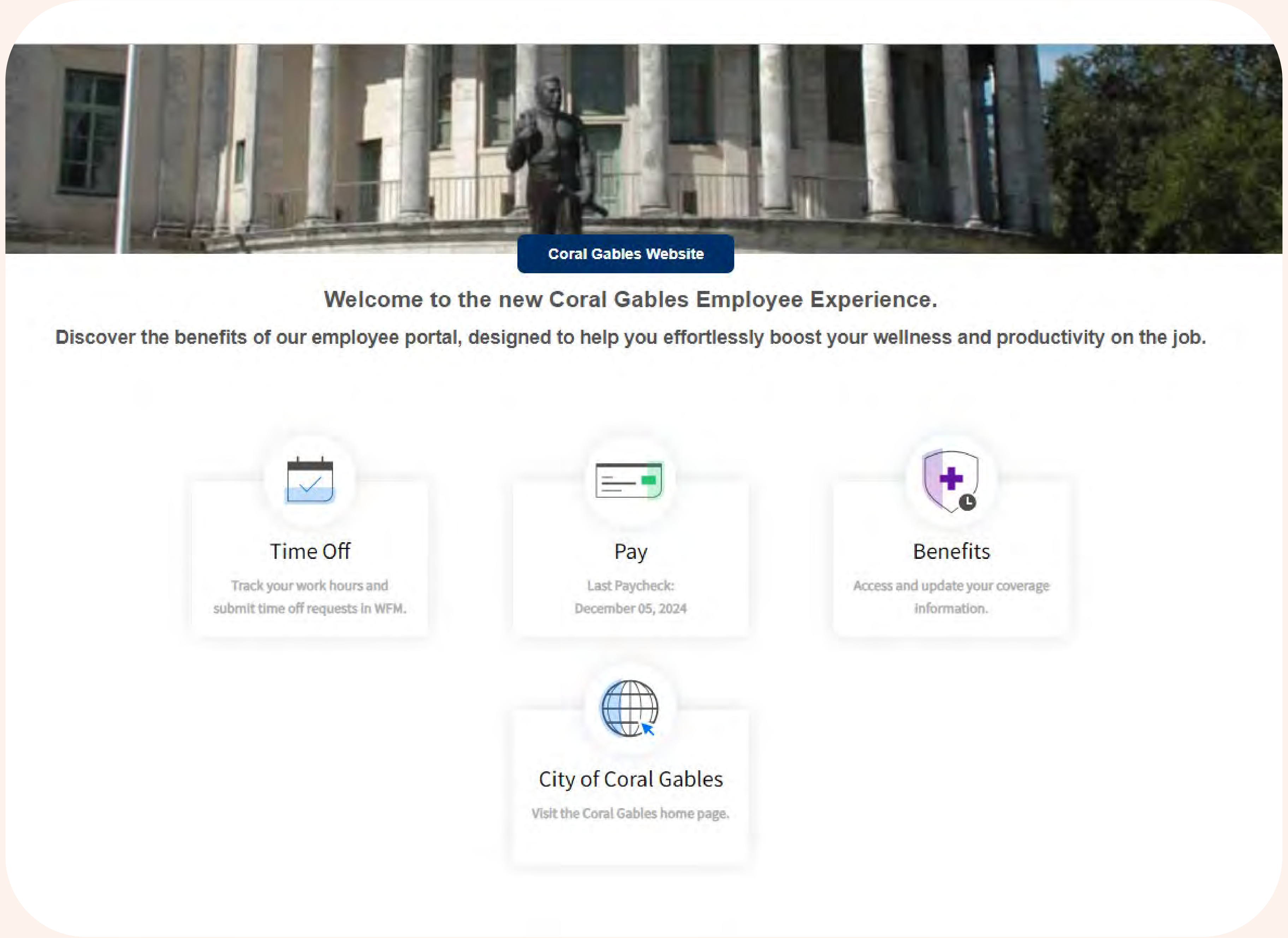
Pay

Benefits

Time Off

Growth

Resources



Coral Gables Website

Welcome to the new Coral Gables Employee Experience.

Discover the benefits of our employee portal, designed to help you effortlessly boost your wellness and productivity on the job.

Time Off

Track your work hours and submit time off requests in WFM.

Pay

Last Paycheck: December 05, 2024

Benefits

Access and update your coverage information.

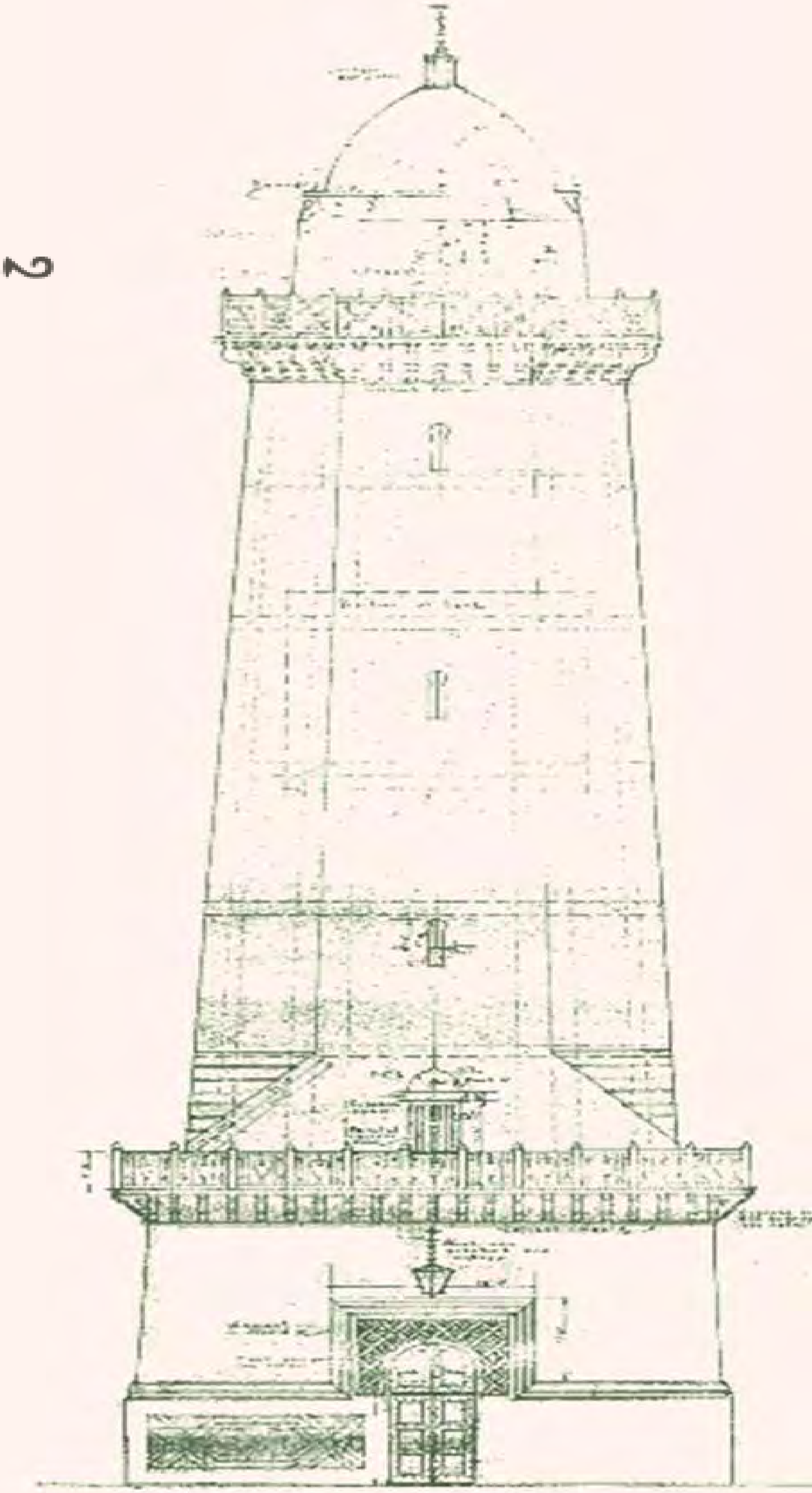
City of Coral Gables

Visit the Coral Gables home page.

In-Service Training

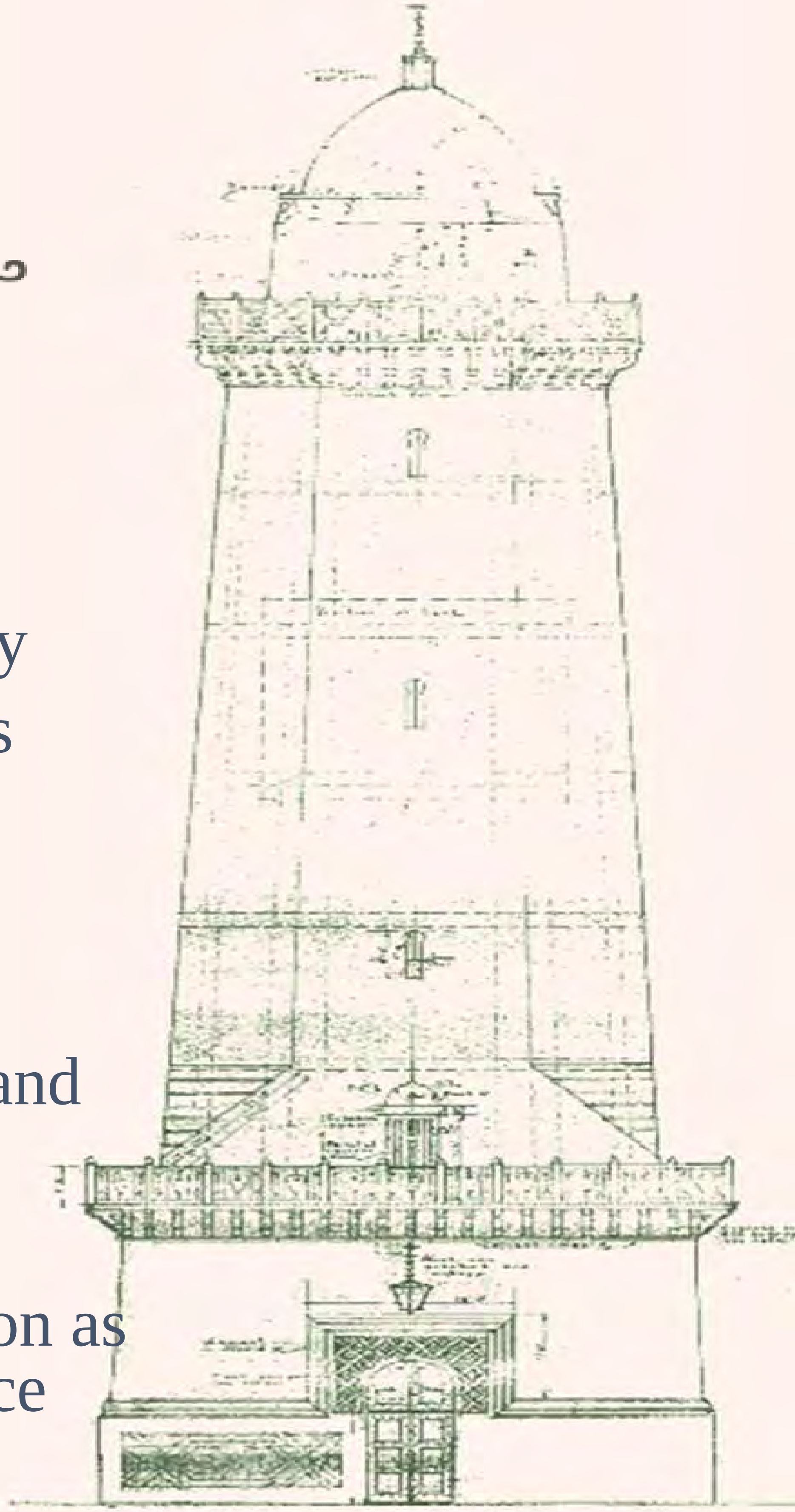
Annual In-Service Training Review

- Law Enforcement & Active Shooter Training
- Emergency Procedures
- Safety Training Handbooks
- Customer Service Training
- Maintenance Standards
- Positive Work Environment & Ethics



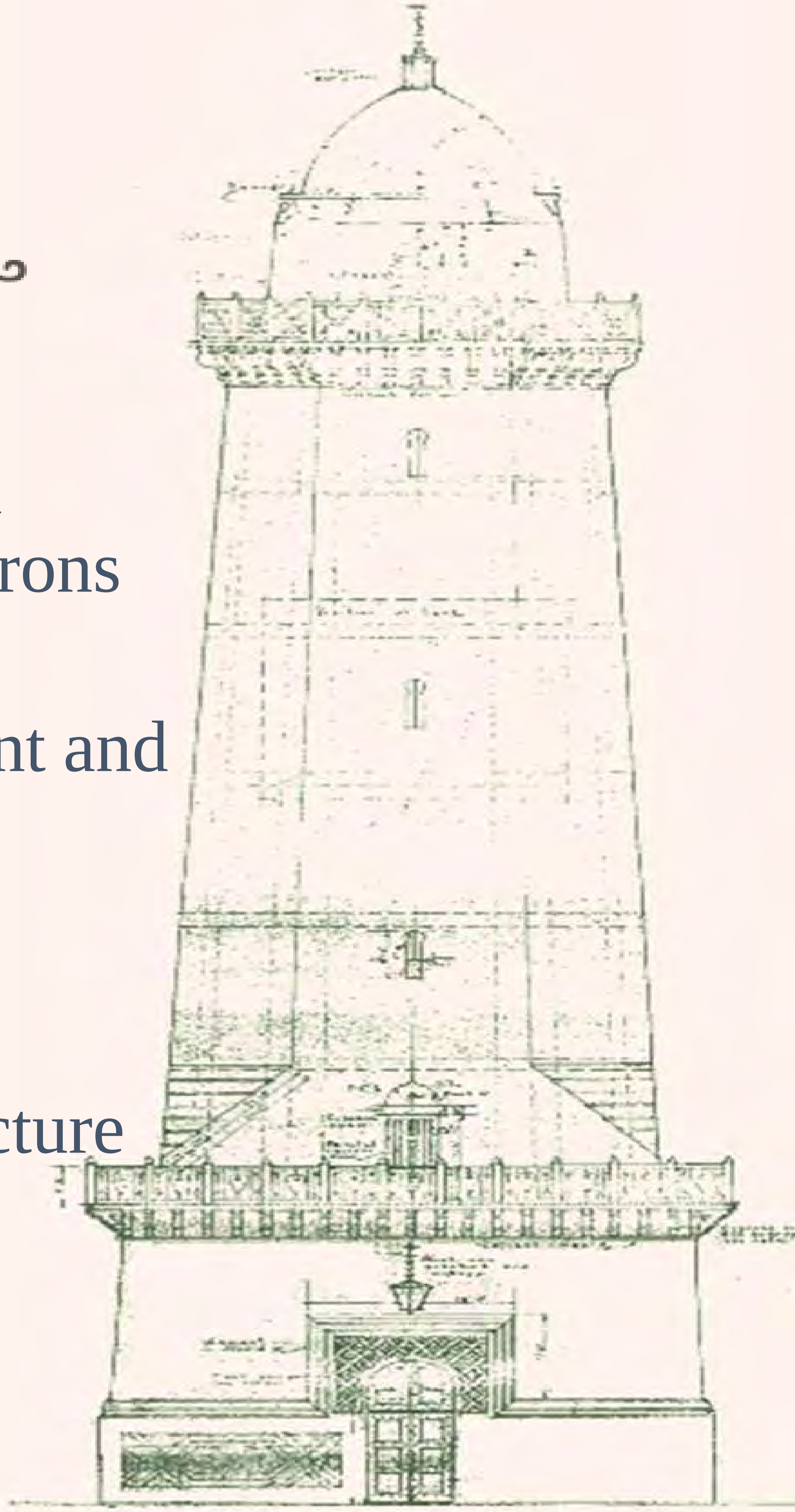
LAW ENFORCEMENT TRAINING

- DEPARTMENT & FACILITY SAFETY PLANS
  - Know your Facility Safety Plans
- FACILITY BUILDING PLANS
  - Know your entry points – limit to a single point of entry
  - Know your emergency exits for evacuation & fire drills
- MONITOR ENTRY & EXIT POINTS
  - Keep doors looked from exterior access
- CAMERA SURVEILLANCE
  - All public areas should be monitored, including fields and parking lots.
- INTERCOM COMMUNICATION SYSTEMS
  - All facilities should be equipped with an intercom button as well as a landline phone to alert the administrative office and/or police department of any critical incident.



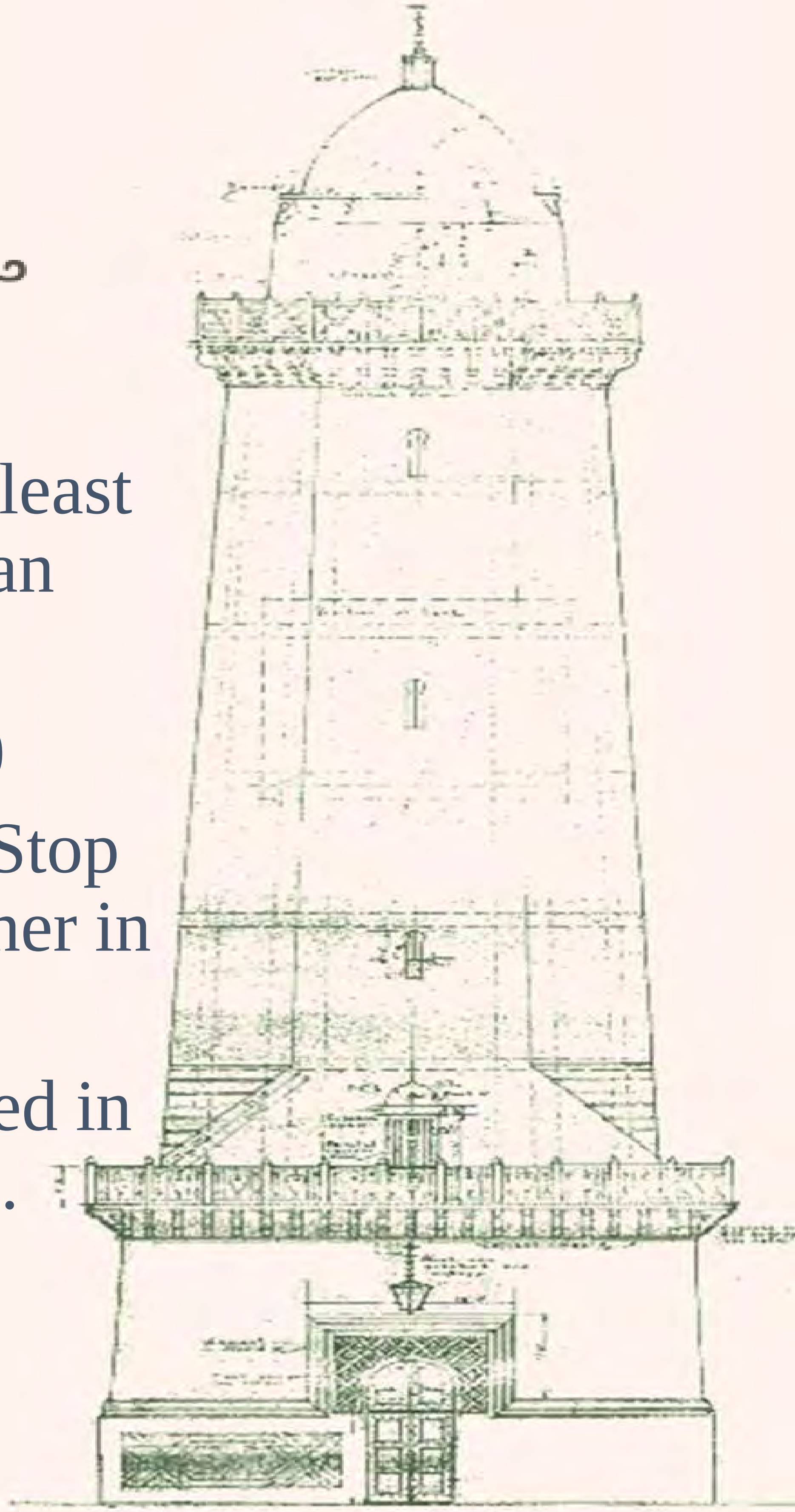
LAW ENFORCEMENT TRAINING

- EMERGENCY NOTIFICATION SYSTEM
  - All facilities should have an emergency notification system to effectively communicate with parents/patrons in the event of a critical incident.
  - This will be used to keep parents updated on relevant and important information.
  - Aftercare example – Procare App
- IDENTIFICATION BADGES
  - It is advisable that all staff and participants wear picture identification badges.
  - They should be visible at all times.



LAW ENFORCEMENT TRAINING

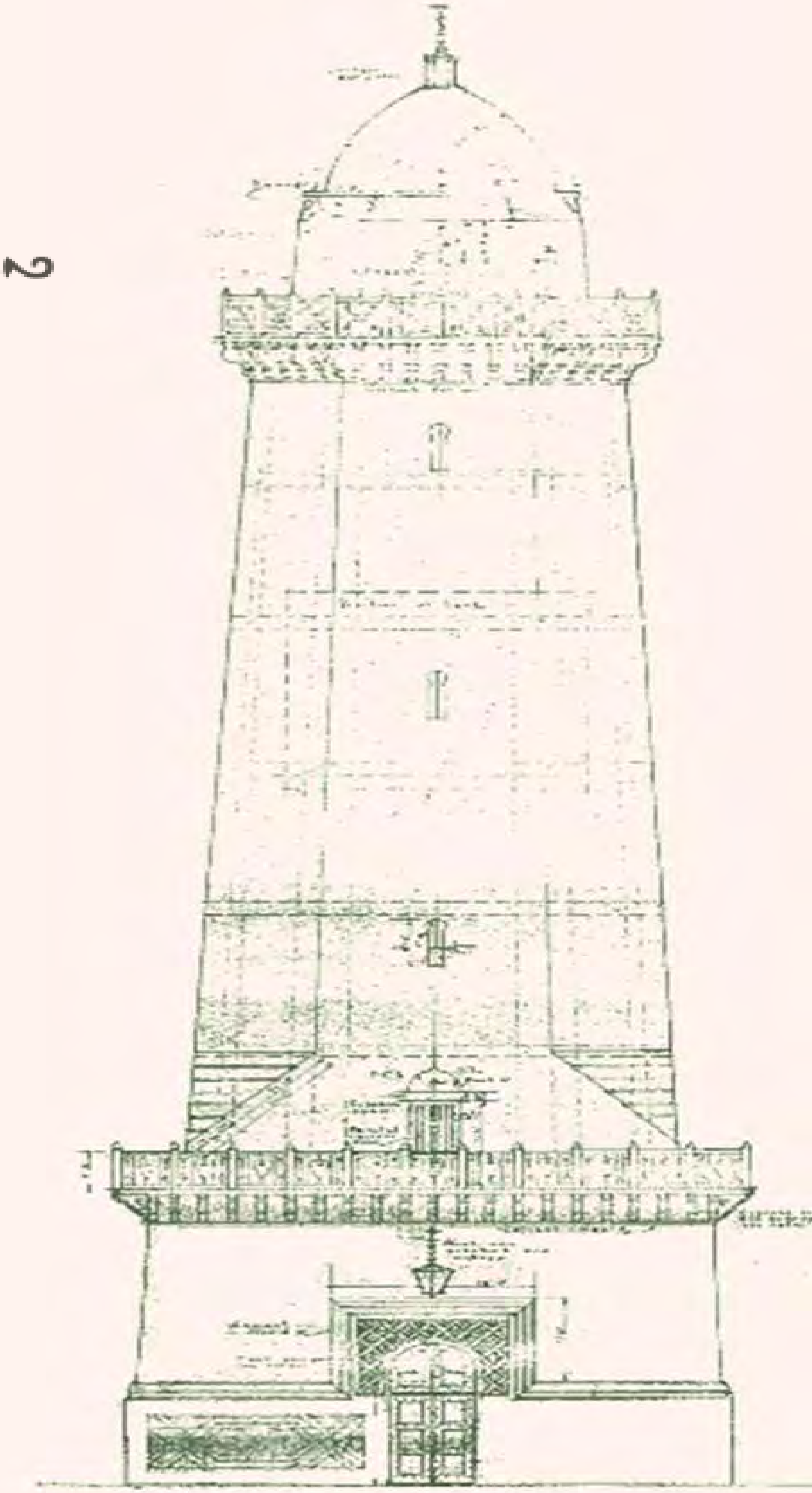
- ACTIVE SHOOTER DRILLS
  - All facilities should conduct active shooter drills at least as often as other emergency drills, but never less than once a year.
- DEFIBRILLATOR AND “STOP THE BLEED” KIT(S)
  - All facilities are equipped with a defibrillator and “Stop the Bleed” kits. These items should be placed together in a visible area and be available to everyone.
  - All staff should be CPR certified and properly trained in the use of a defibrillator and “Stop the Bleed” kit(s).



Law Enforcement Training

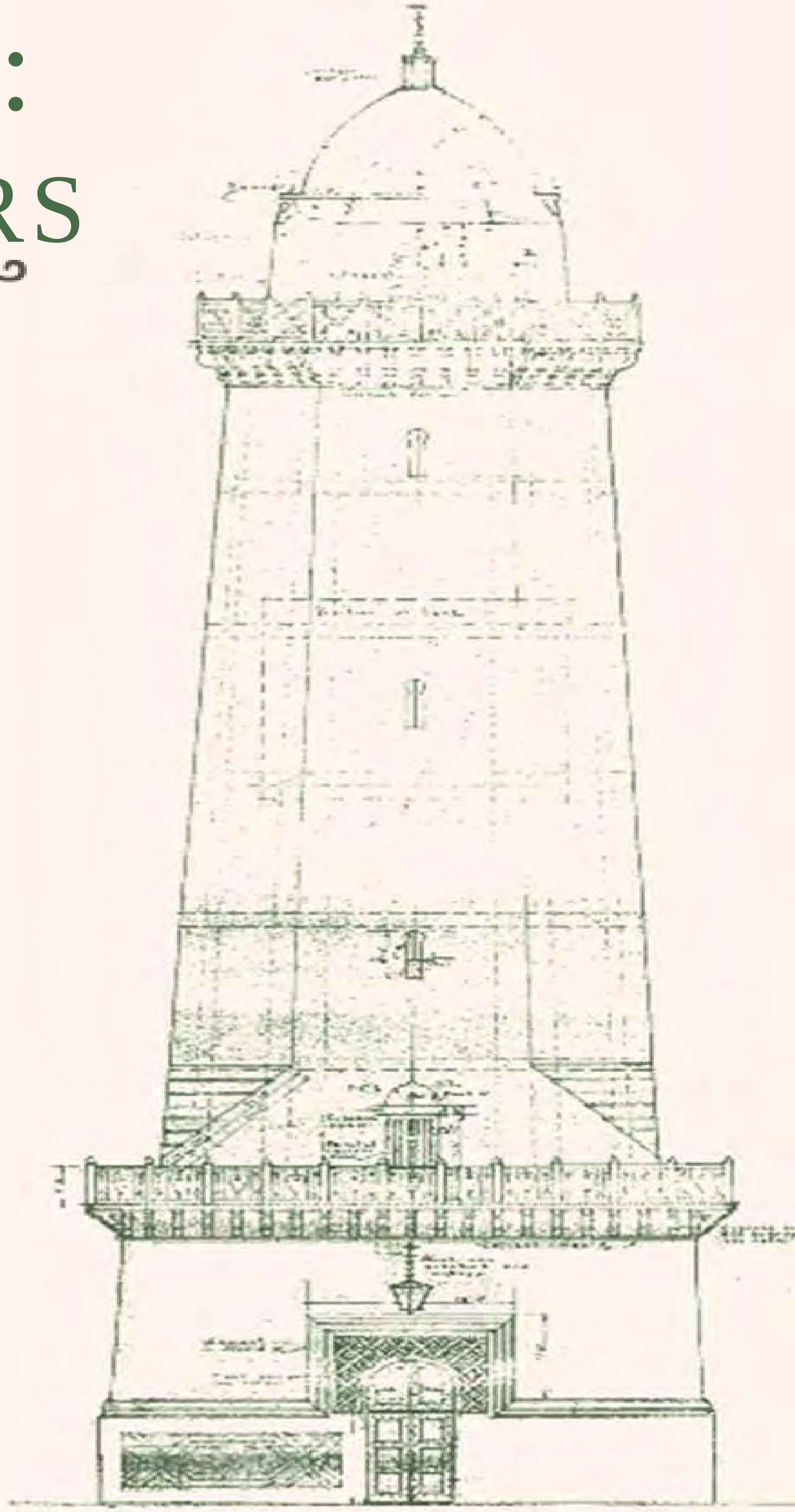
- ACTIVE SHOOTER
  - RUN
  - HIDE
  - FIGHT

- Play *Surviving an Active Shooter Event* Video



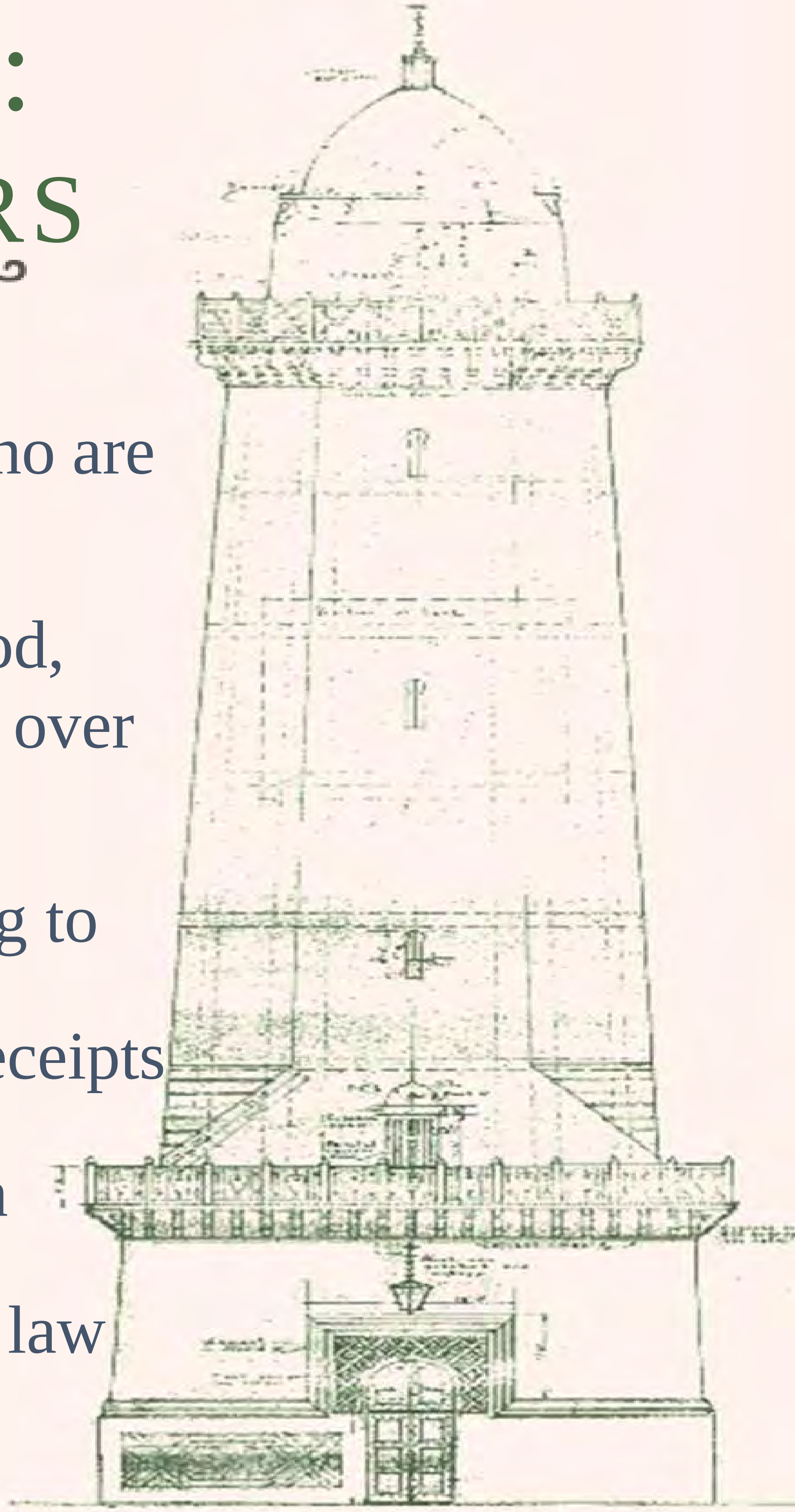
Law Enforcement Training: Potential Attack Indicators

- Individual Behavior Indicators:
  - Socially isolated,
  - Threats of violence against others,
  - Unsolicited focus on dangerous weapons,
  - Unstable emotional responses,
  - Intense anger and hostility,
  - Loss of significant relationships,
  - Feeling either arrogant and supreme, or powerless,
  - Expressions of paranoia or depression,
  - Increased use of alcohol or drugs,
  - Depression or withdrawal,
  - Talk of suicide,
  - Increased absenteeism.



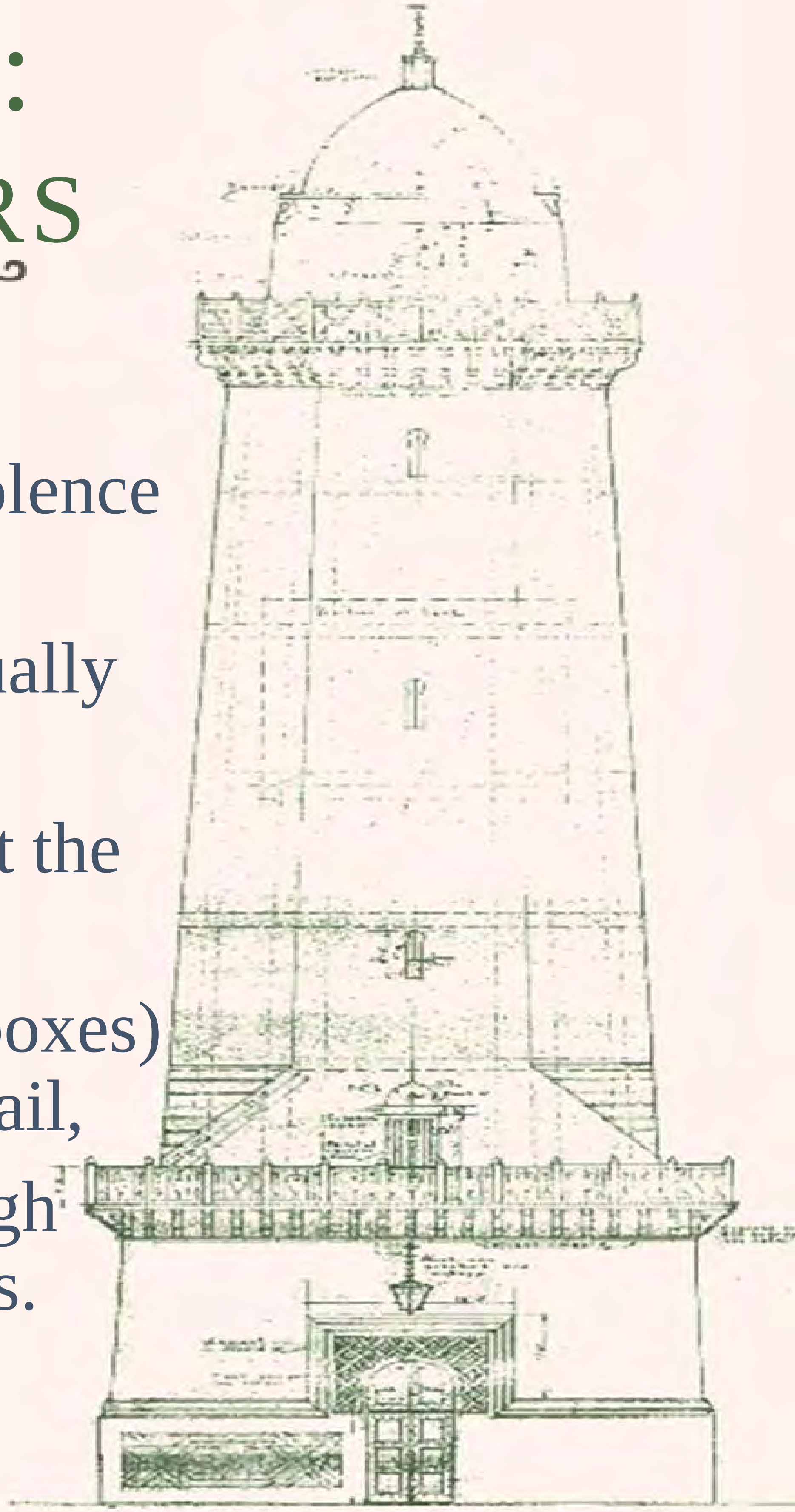
Law Enforcement Training: Potential Attack Indicators

- Surveillance Indicators:
  - Persons attempting to gain access into the facility or who are located in the building with no legitimate purpose,
  - Persons using or carrying video/camera/observation equipment in or near the facility over an extended period,
  - Persons parking, standing, or loitering in the same area over a multiple-day period with no apparent reasonable explanation,
  - Persons excessively inquiring about practices pertaining to the facility and its operations,
  - Persons observed or reported to be observing facility receipts or deliveries,
  - Threats by telephone, mail, or e-mail and/or increase in reports of threats from known reliable sources,
  - A noted pattern of false alarms requiring a response by law enforcement or emergency services.



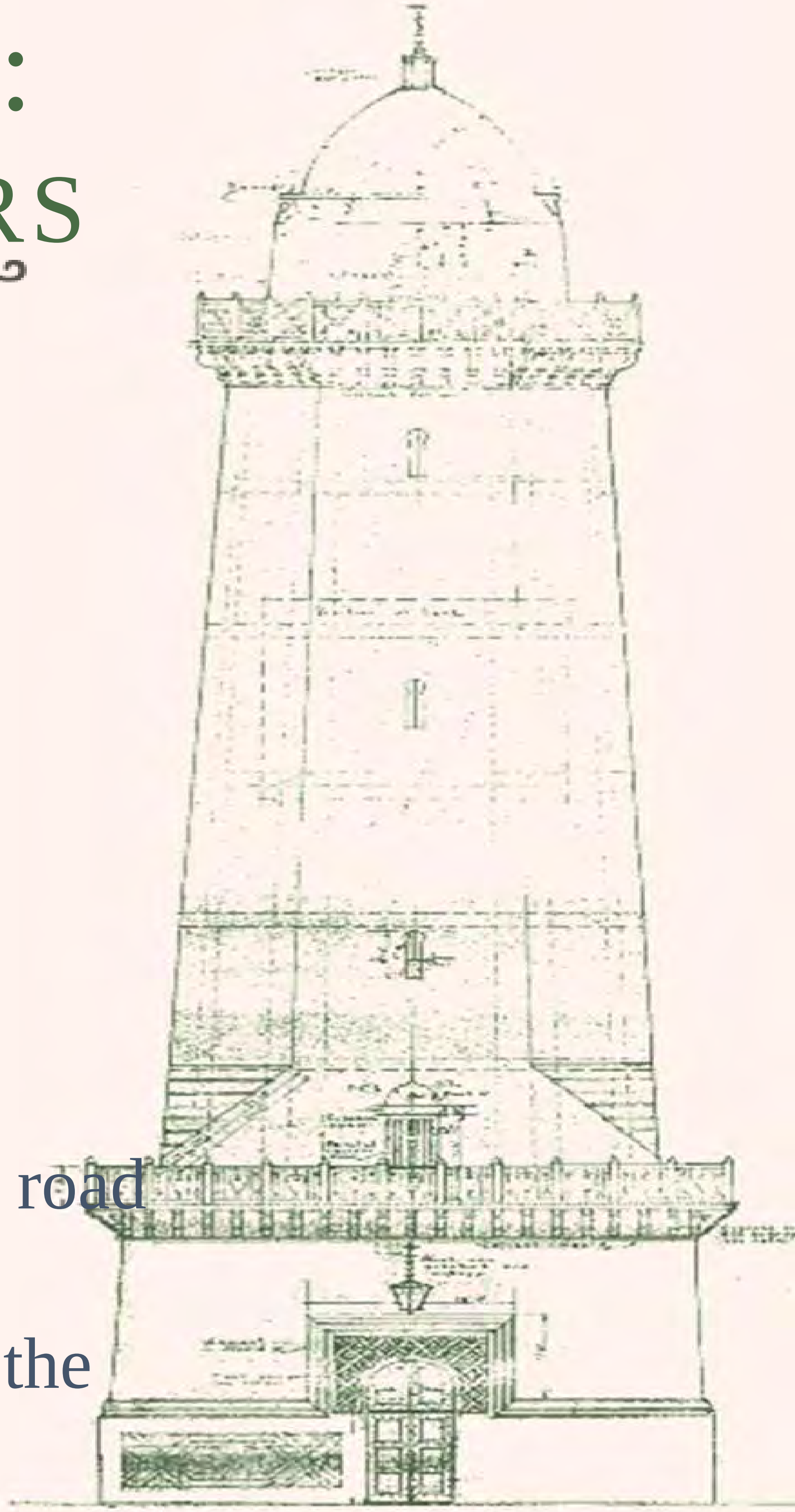
Law Enforcement Training: Potential Attack Indicators

- Imminent Attack Indicators:
  - Reports from staff about a coworker threatening violence that includes specific dates/times/locations/targets,
  - Suspicious persons in crowded areas wearing unusually bulky clothing that might conceal explosives,
  - Unexpected or unfamiliar delivery trucks arriving at the facility,
  - Unattended packages (e.g., backpacks, briefcases, boxes) or suspicious packages and/or letters received by mail,
  - Vehicles approaching the facility at an unusually high speed or steering around barriers and traffic controls.



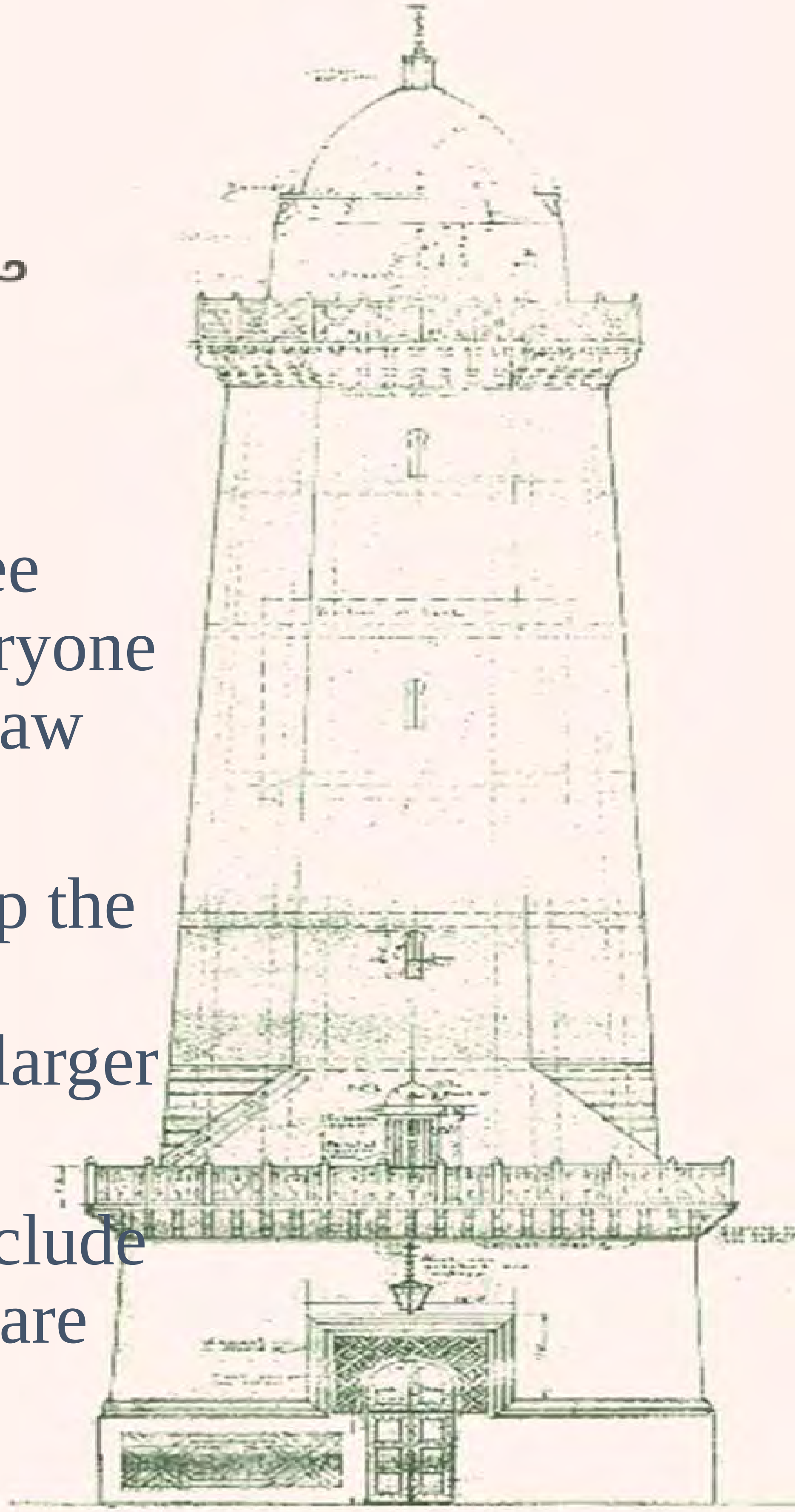
Law Enforcement Training: Potential Attack Indicators

- Surrounding Area Indicators:
  - An increase in reporting of buildings being left unsecured or doors left unlocked, when they are normally secured and locked at all times,
  - Theft or unauthorized possession of employee identification cards, uniforms, or security communications,
  - Unfamiliar contract workers attempting to access unauthorized areas,
  - Unusual or unexpected maintenance activities (e.g., road repairs) near the facility,
  - Sudden increases in power outages designed to test the backup systems or recovery times.



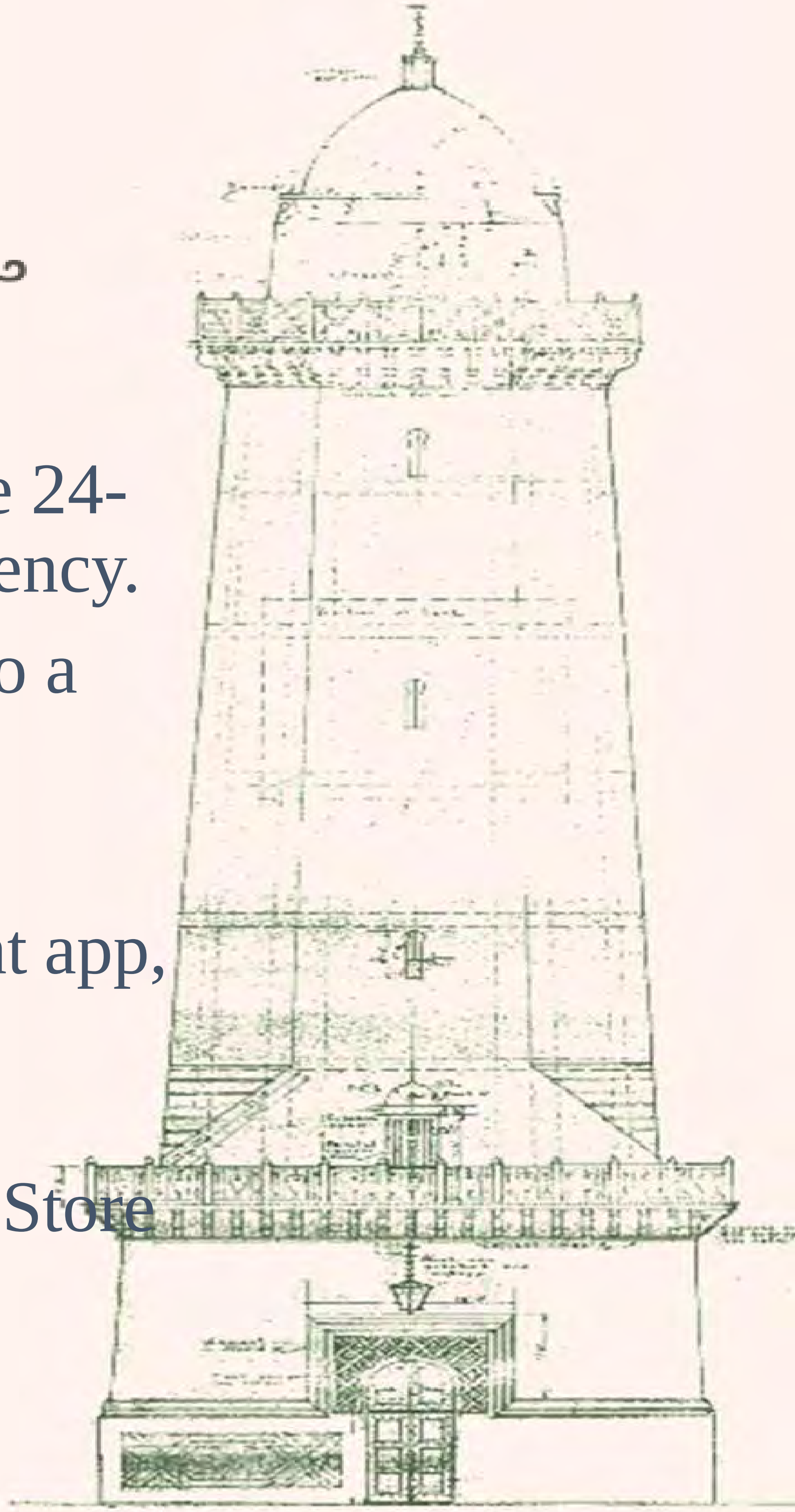
Law Enforcement Training

- “SEE SOMETHING, SAY SOMETHING”
  - All facilities should initiate “See Something, Say Something” protocols for staff and patrons. The “See Something, Say Something” campaign benefits everyone by bringing suspicious behavior to the attention of law enforcement.
  - Reporting suspicious behavior could potentially stop the next terrorist incident. “Even if you think your observation is not important, it may be a piece of a larger puzzle.”
- Participants are provided with parent handbooks that include safety protocol and prevention information so that they are included as part of the security team.



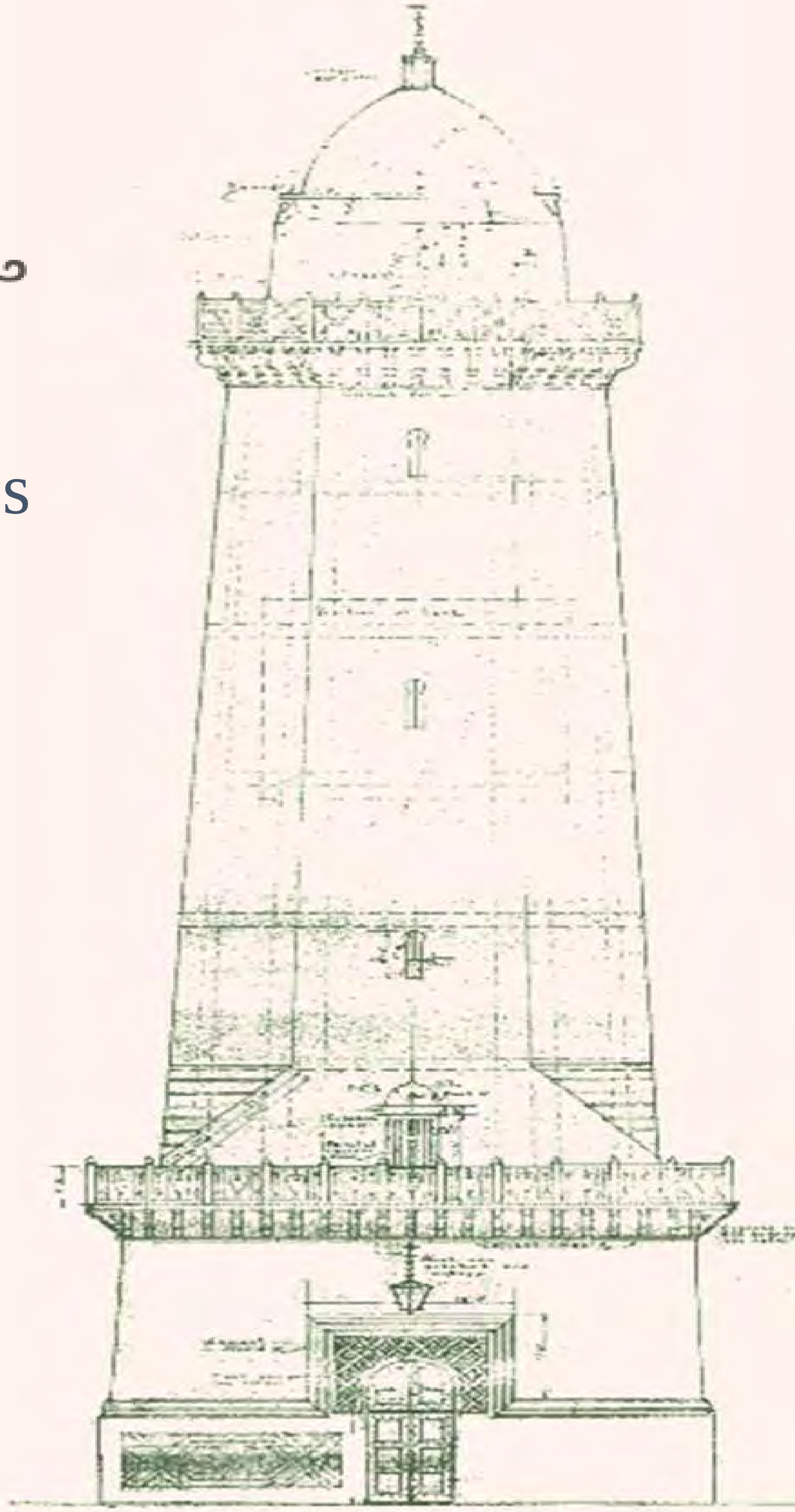
Law Enforcement Training

- FIRST RESPONDER ACCESS TO THE FACILITY
    - The Coral Gables Police and Fire Departments have 24-hour access to all facilities in the event of an emergency.
    - After hours this may be accomplished with access to a traditional key or code via a building lock box.
- IN-TELLIGENT APP
    - By downloading and registering with the In-telligent app, you will receive public safety alerts from the Coral Gables Police Department.
    - The app can be downloaded from the Apple iTunes Store or Google Play Store.

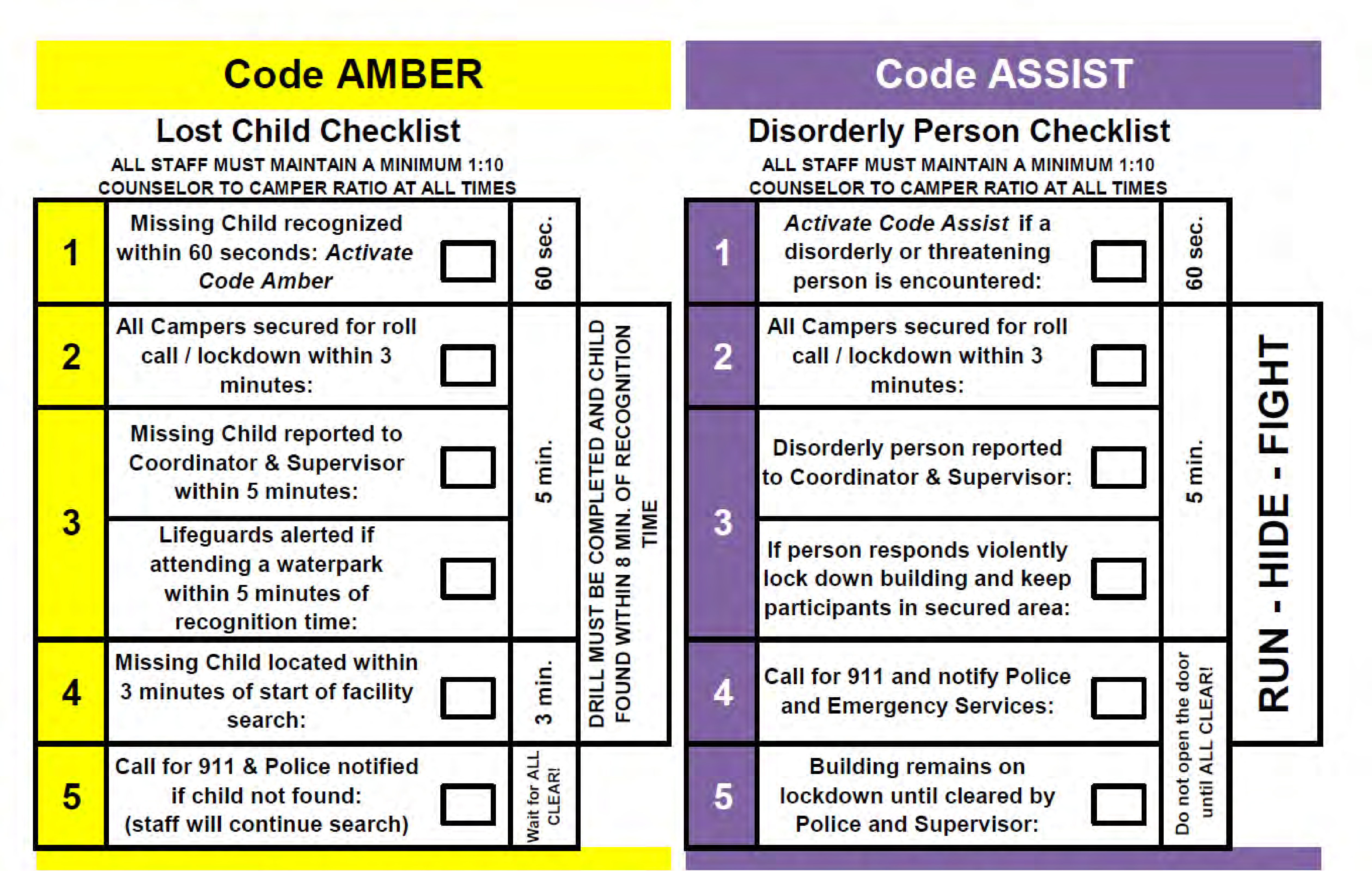


Law Enforcement Training

- BASIC INCIDENT RECOVERY
  - Assemble a Crisis Intervention Team (cit) and assess emotional needs of staff, students, facilities, and responders.
  - Keep students, families, and the media informed.
  - Return to business as quickly as possible
  - Provide stress management as needed
  - Restore infrastructure
  - Evaluate & make recommended changes



Law Enforcement Training: Emergency Codes



Code AMBER

Lost Child Checklist

ALL STAFF MUST MAINTAIN A MINIMUM 1:10 COUNSELOR TO CAMPER RATIO AT ALL TIMES

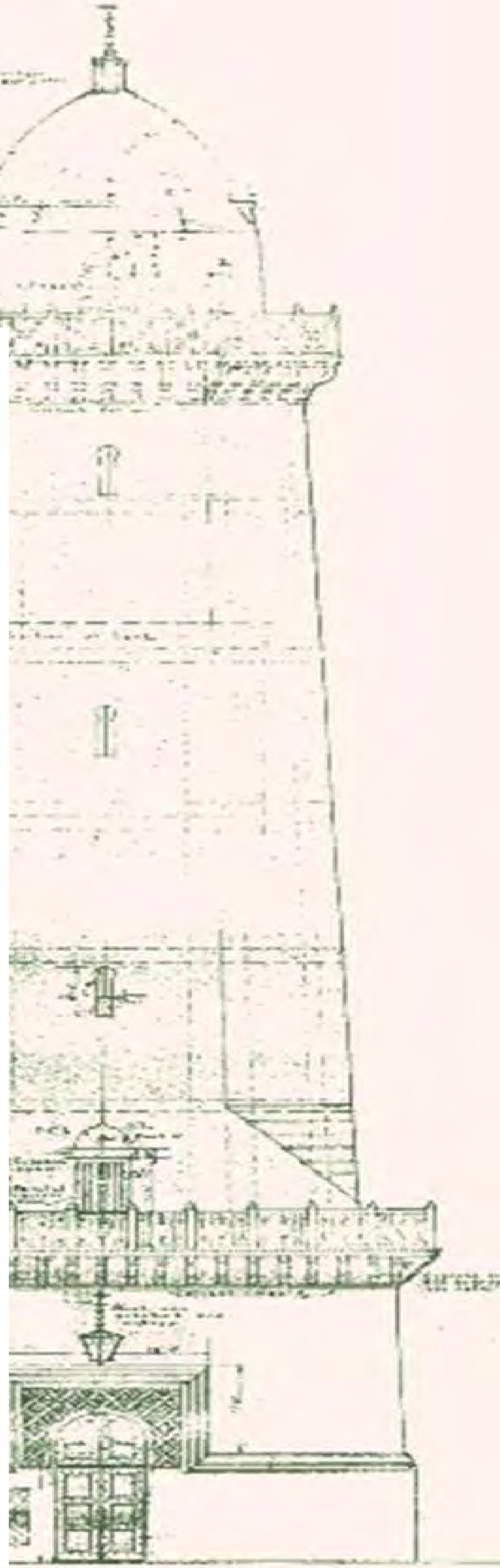
1	Missing Child recognized within 60 seconds: *Activate Code Amber*	□	60 sec.	
2	All Campers secured for roll call / lockdown within 3 minutes:	□	5 min.	DRILL MUST BE COMPLETED AND CHILD FOUND WITHIN 8 MIN. OF RECOGNITION TIME
3	Missing Child reported to Coordinator & Supervisor within 5 minutes:	□		
	Lifeguards alerted if attending a waterpark within 5 minutes of recognition time:	□		
4	Missing Child located within 3 minutes of start of facility search:	□	3 min.	
5	Call for 911 & Police notified if child not found: (staff will continue search)	□	Wait for ALL CLEAR!	

Code ASSIST

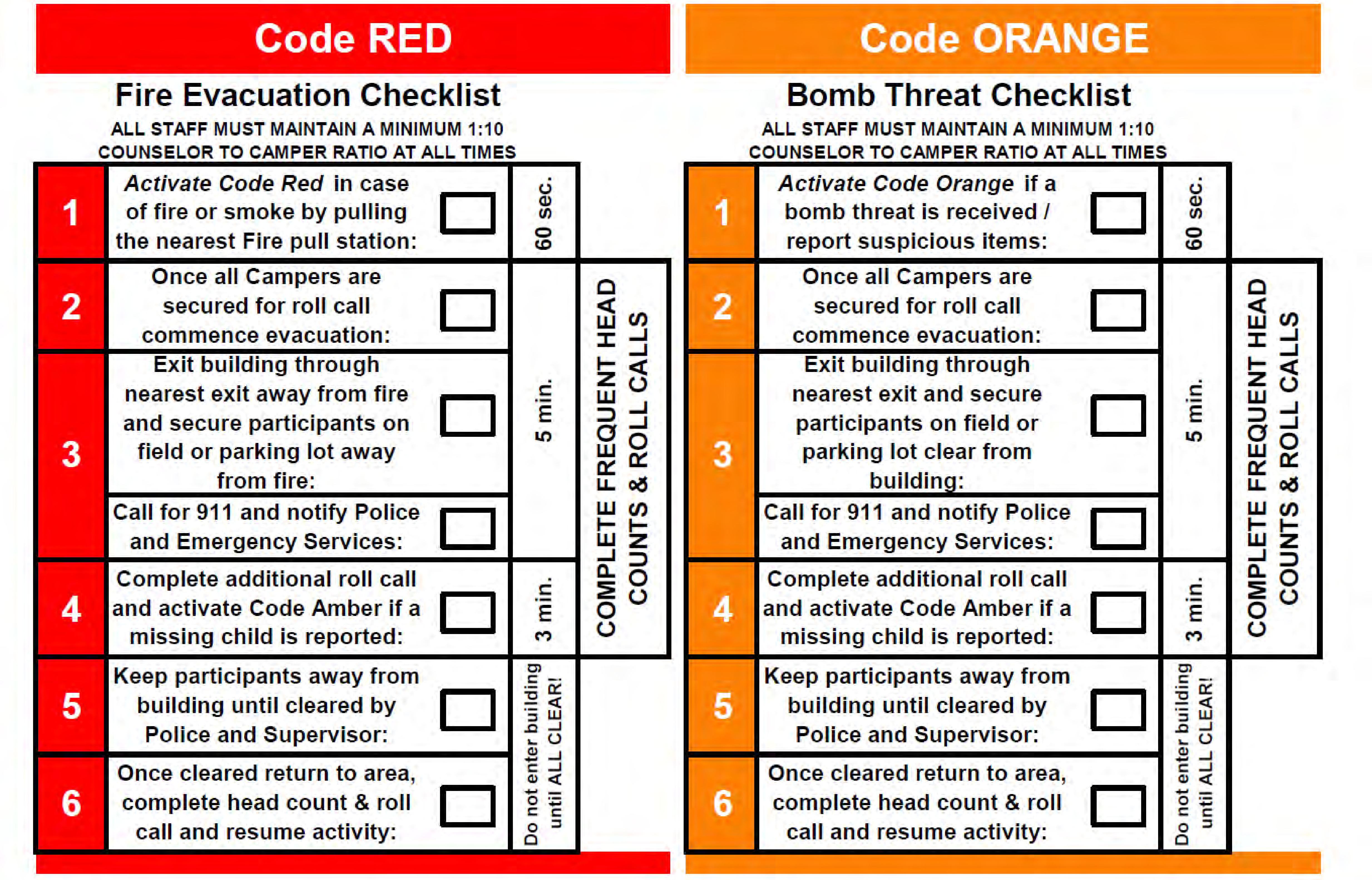
Disorderly Person Checklist

ALL STAFF MUST MAINTAIN A MINIMUM 1:10 COUNSELOR TO CAMPER RATIO AT ALL TIMES

1	*Activate Code Assist* if a disorderly or threatening person is encountered:	□	60 sec.	
2	All Campers secured for roll call / lockdown within 3 minutes:	□	5 min.	RUN - HIDE - FIGHT
3	Disorderly person reported to Coordinator & Supervisor:	□		
	If person responds violently lock down building and keep participants in secured area:	□		
4	Call for 911 and notify Police and Emergency Services:	□	Do not open the door until ALL CLEAR!	
5	Building remains on lockdown until cleared by Police and Supervisor:	□		



Law Enforcement Training: Emergency Codes



Code RED

Fire Evacuation Checklist

ALL STAFF MUST MAINTAIN A MINIMUM 1:10 COUNSELOR TO CAMPER RATIO AT ALL TIMES

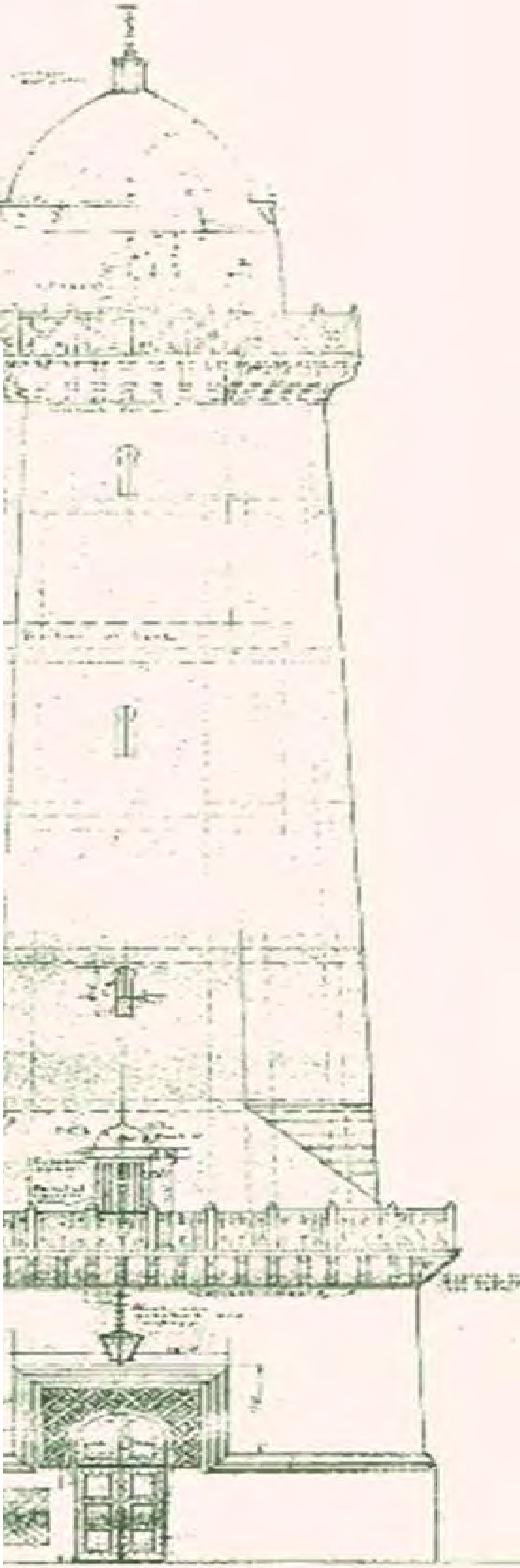
1	*Activate Code Red* in case of fire or smoke by pulling the nearest Fire pull station:	□	60 sec.	
2	Once all Campers are secured for roll call commence evacuation:	□	5 min.	COMPLETE FREQUENT HEAD COUNTS & ROLL CALLS
3	Exit building through nearest exit away from fire and secure participants on field or parking lot away from fire:	□		
	Call for 911 and notify Police and Emergency Services:	□		
4	Complete additional roll call and activate Code Amber if a missing child is reported:	□	3 min.	
5	Keep participants away from building until cleared by Police and Supervisor:	□	Do not enter building until ALL CLEAR!	
6	Once cleared return to area, complete head count & roll call and resume activity:	□		

Code ORANGE

Bomb Threat Checklist

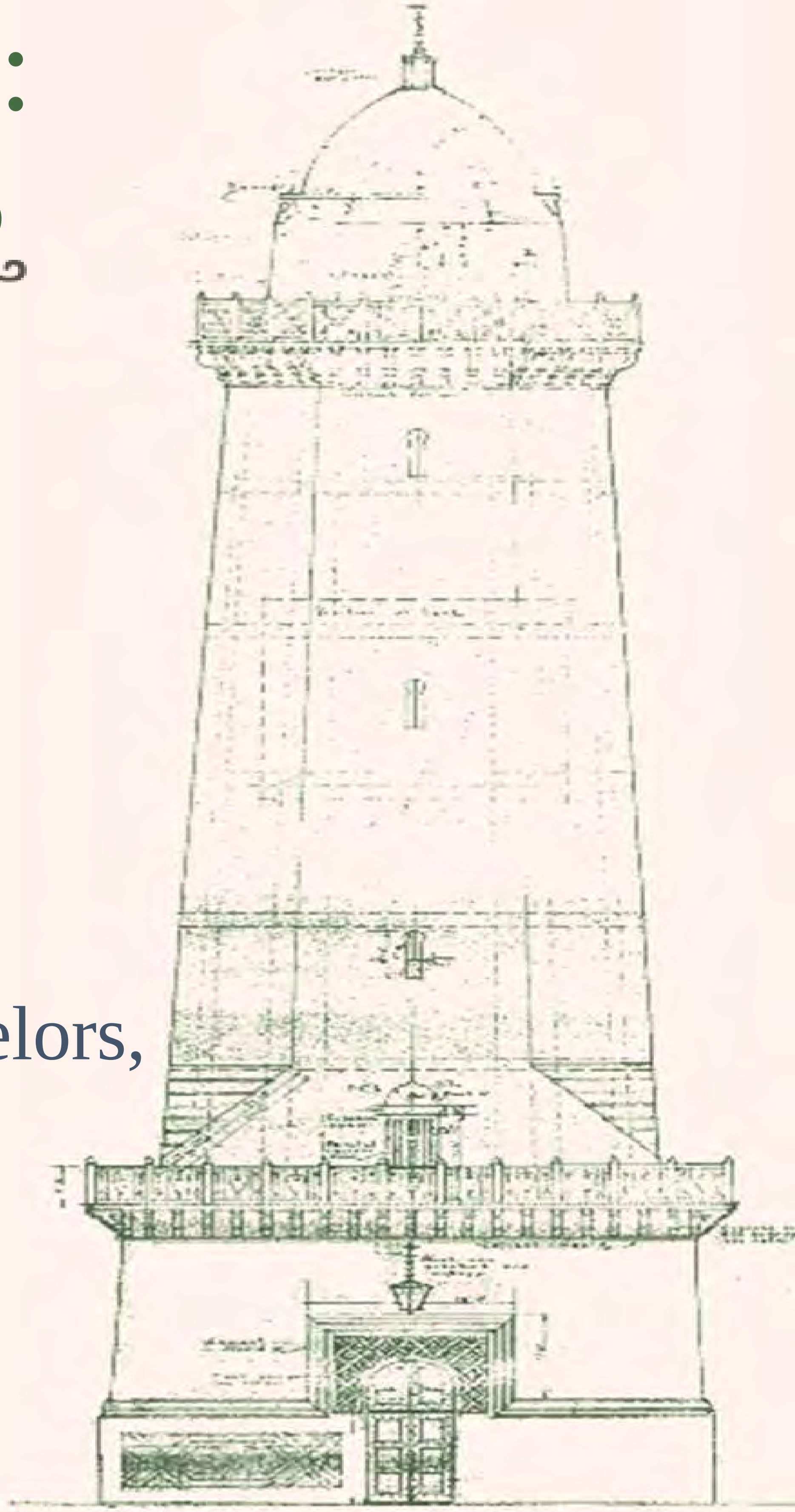
ALL STAFF MUST MAINTAIN A MINIMUM 1:10 COUNSELOR TO CAMPER RATIO AT ALL TIMES

1	*Activate Code Orange* if a bomb threat is received / report suspicious items:	□	60 sec.	
2	Once all Campers are secured for roll call commence evacuation:	□	5 min.	COMPLETE FREQUENT HEAD COUNTS & ROLL CALLS
3	Exit building through nearest exit and secure participants on field or parking lot clear from building:	□		
	Call for 911 and notify Police and Emergency Services:	□		
4	Complete additional roll call and activate Code Amber if a missing child is reported:	□	3 min.	
5	Keep participants away from building until cleared by Police and Supervisor:	□	Do not enter building until ALL CLEAR!	
6	Once cleared return to area, complete head count & roll call and resume activity:	□		



Law Enforcement Training: P&R SAFETY HANDBOOKS

- City Safety Manual
- Risk Management Plan
- Vehicle Safety Manual
- Playground Safety Manual
- Golf Grounds & Maintenance Safety Manual
- Emergency Procedures – Guest Services, Counselors, Park Rangers and Lifeguards
- Emergency Contact Flowchart
- Workers Compensation



Trivia Question #6

What is the website address for the Community Recreation Page?

Correct Answer to Question #6

GABLESRECREATION.COM

Providing Exceptional Customer Service

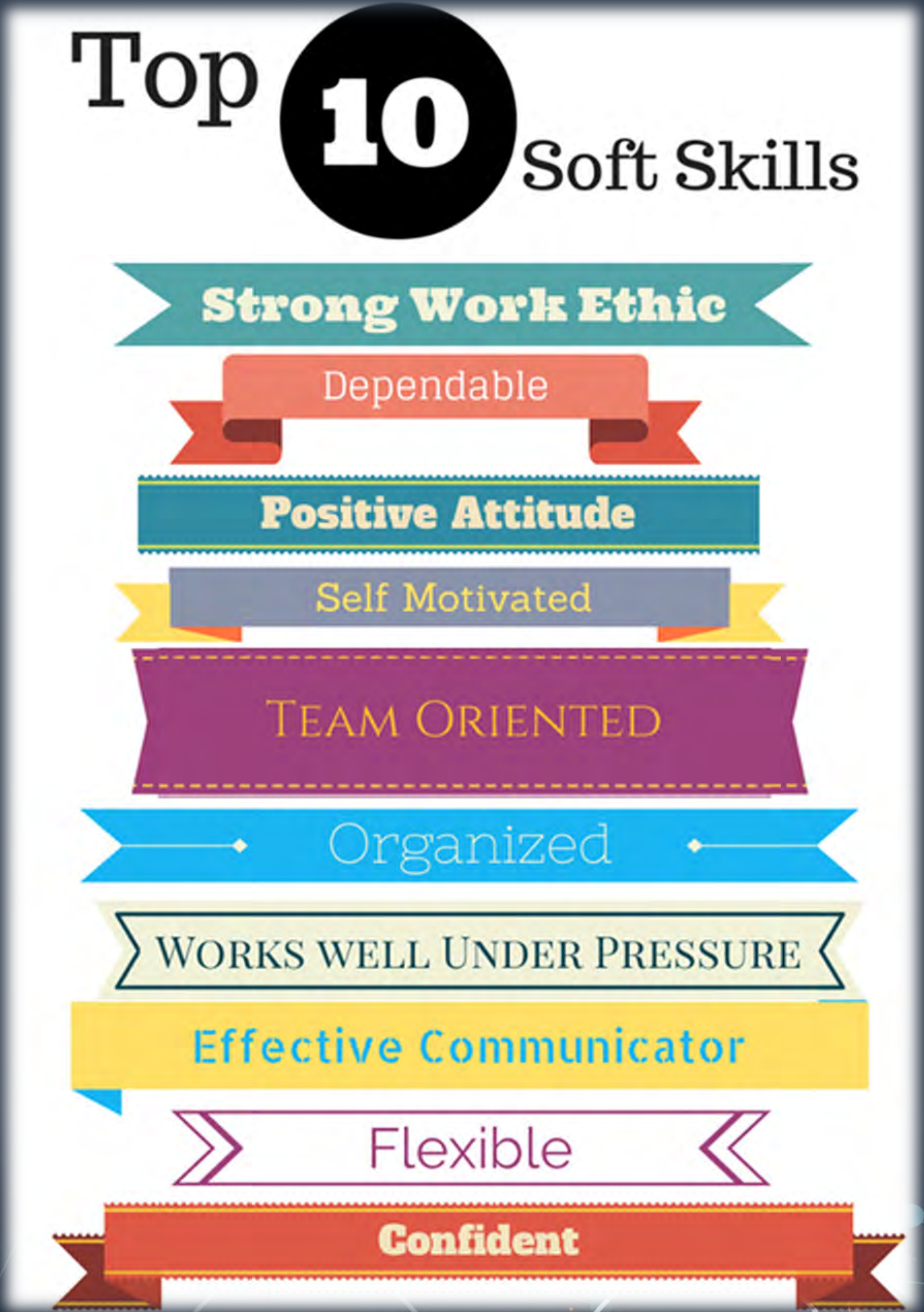
10 Tools To Create An Exceptional Guest Experience

Service Matters To Our Guests…

#1 Recruitment & Training

Employee Investment:
Our employees are your business ambassadors…and our brand!

#1 Recruitment & Training



Top 10 Soft Skills

- Strong Work Ethic
- Dependable
- Positive Attitude
- Self Motivated
- Team Oriented
- Organized
- Works Well Under Pressure
- Effective Communicator
- Flexible
- Confident

While we traditionally hire for hard skills…look to hire for soft skills instead.

Hire for attitude and train for skills!

#1 Recruitment & Training

Train, Train & Train again!

- Onboarding
- Employee Manual
- Ongoing Training & In-Services
- Development & Growth Opportunities

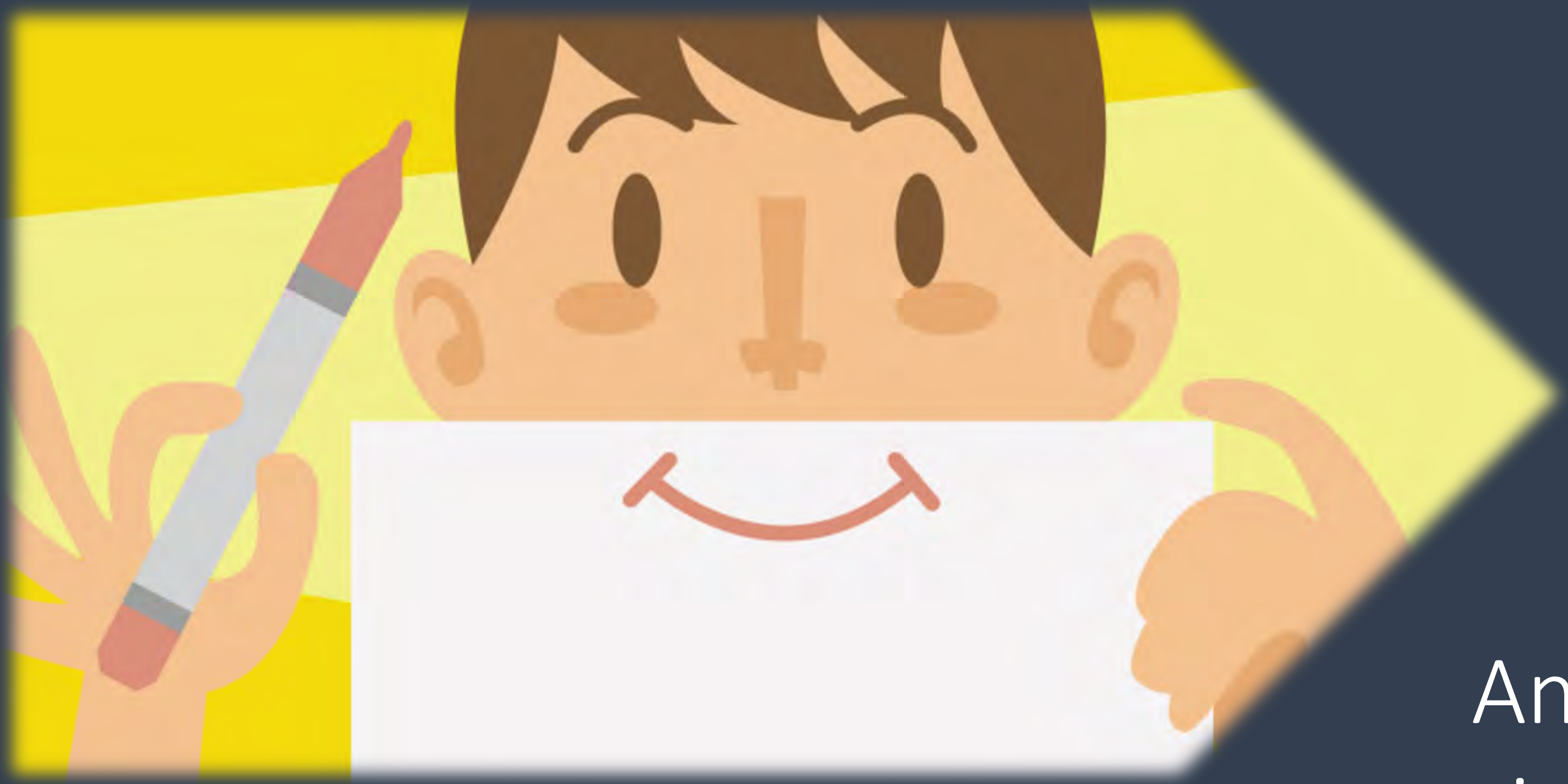
#1 Recruitment & Training

Breakout Assignment:

Discuss amongst your group what type of soft skills you look for during the recruitment process.

#2 Smile…

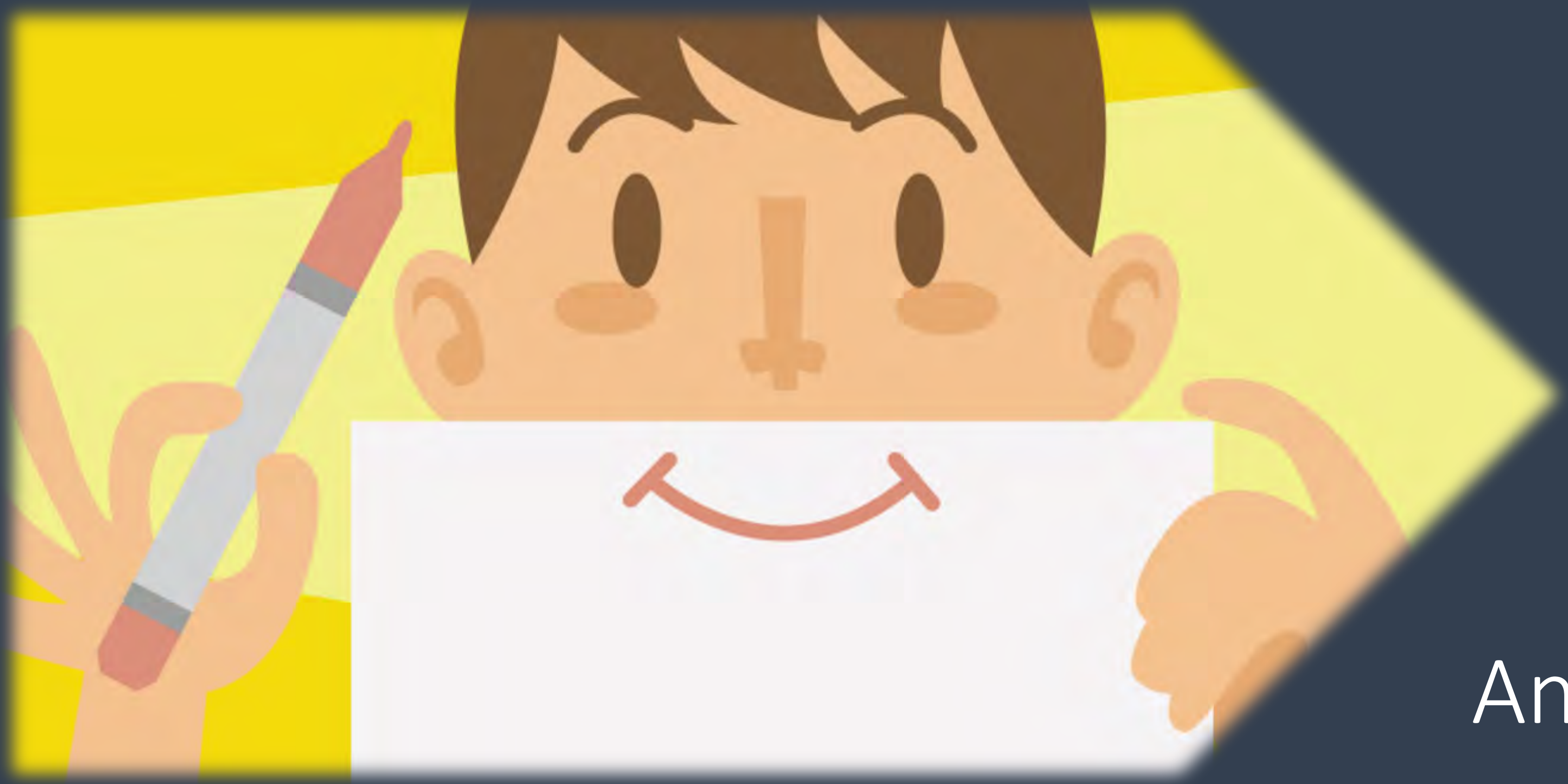
Back to the Basics



An employee’s smile may be the most significant part of a transaction.

Did you know that Smiling while speaking can change the tone in your voice?

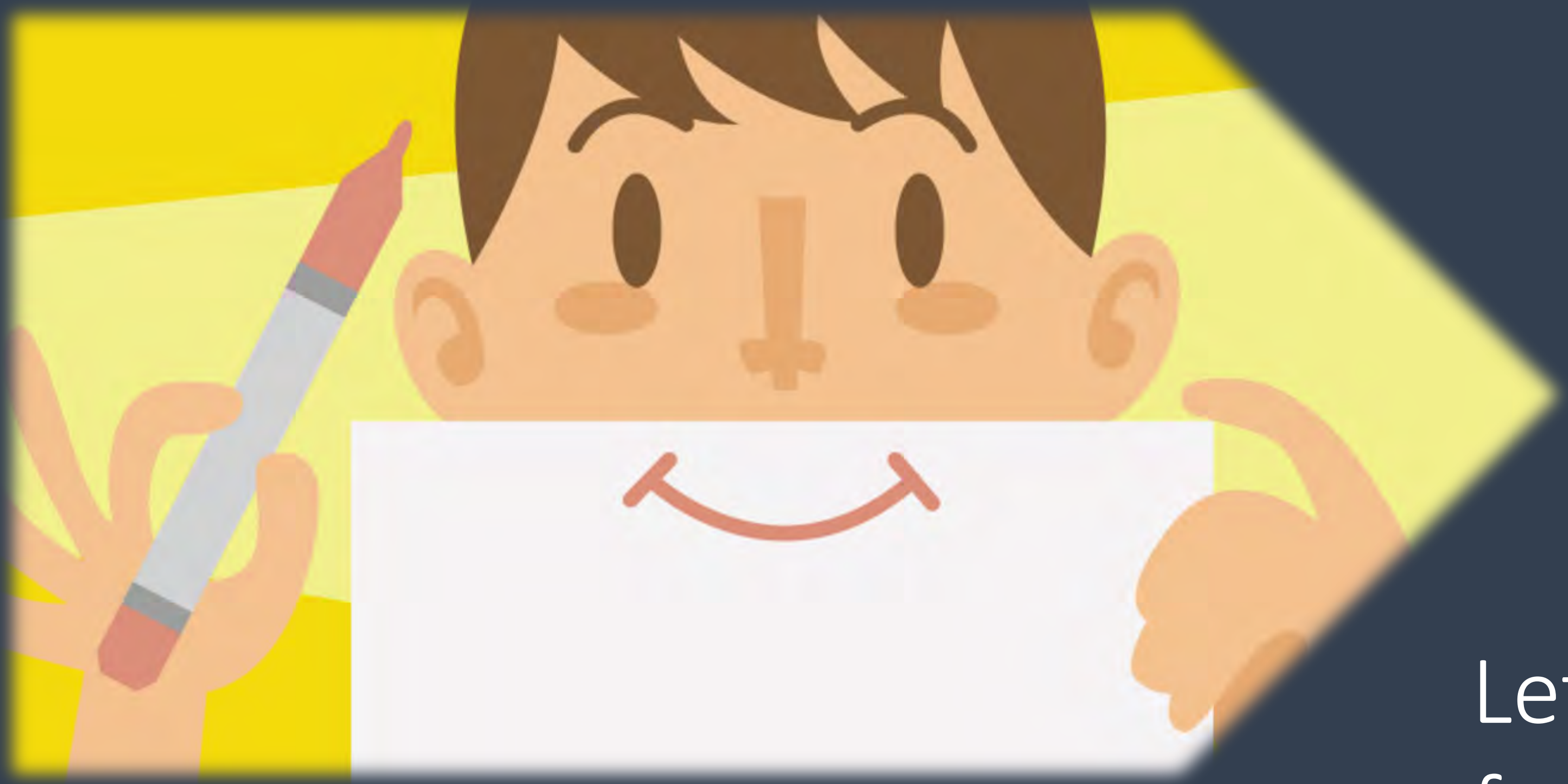
#2 Smile…
Back to the Basics



An initial smile may set the tone for the remainder of the transaction!

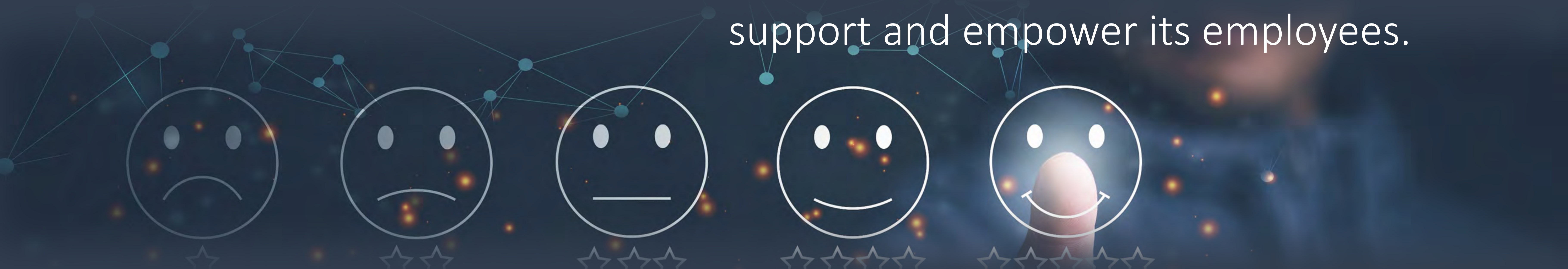
Plus, happy employees are proven to be more productive employees.

#2 Smile…
Back to the Basics



Let’s be clear: service with a smile isn’t forced on employees.

It should be a natural consequence of an organization that understands how to support and empower its employees.



#3 Happy Employees = Happy Customers

The key to achieving customer happiness, as in customers who want to do business with you again and again, is to focus on employee happiness first.

#3 Happy Employees = Happy Customers

Did you know that a happy staff improves employee engagement & retention!

And the longer a staff member stays the more knowledgeable they become of the organization and its services – resulting in better quality interactions with your customers.

#3 Happy Employees = Happy Customers

So what can you do to keep your employees happy?

- Provide meaning to their job
- Show your employees they are supported…from the top down
- Create a fun work environment
- Provide recognition and feedback

#4 10/5
Greeting Rule

Popular practice in the hospitality & service industry.

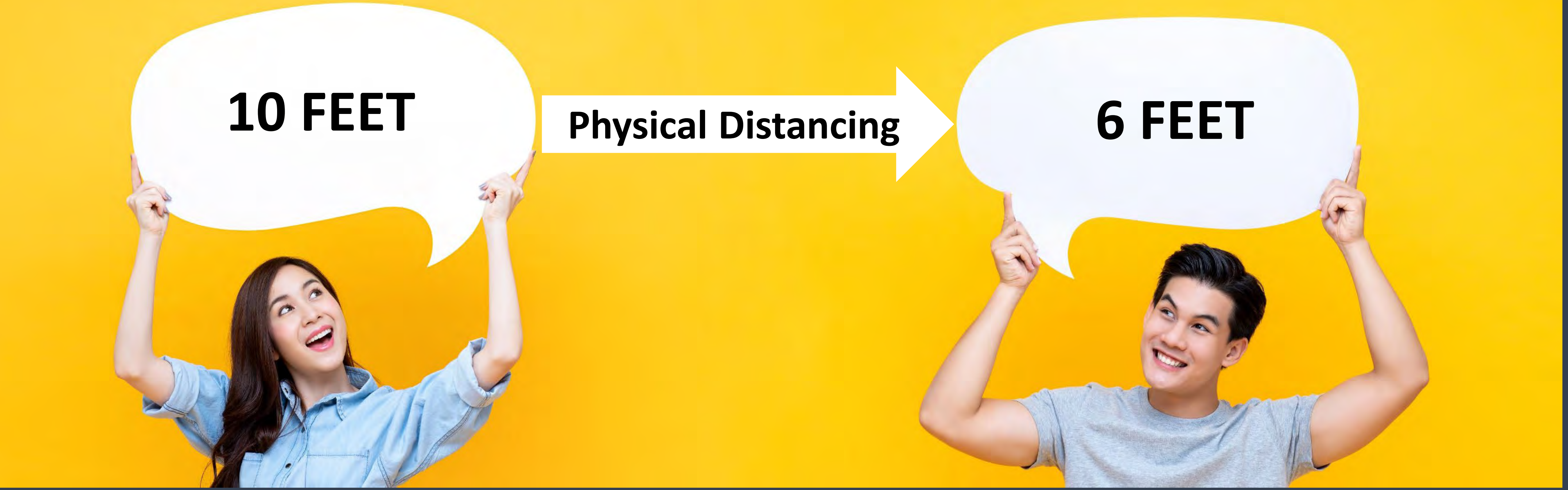
When you are within ten feet of a customer you attempt to make eye contact and smile to greet the approaching patron.

#4 10/5 Greeting Rule

When you are within five feet, you acknowledge them verbally with a "Hello," "Good Morning/Afternoon/Evening".

Use the customer's name after it's been given whenever the opportunity arises.

#4 10/5 Greeting Rule



<u>Give it a try with a physical distancing twist:</u>

Greeting at 10 feet

Greeting at 6 feet

#5 Identify Customer Needs

Customer needs are the named and unnamed needs your customer has when they come into contact with your business, your competitors, or when they search for the solutions you provide.

#5 Identify Customer Needs

All customers have two needs: A service and a psychological need.

To identify the needs of your customers, solicit feedback from your customers at every step of your process.

#5 Identify Customer Needs

Top 6 Basic Customer Needs:

- Friendliness
- Understanding & Empathy
- Fairness
- Control
- Options & Alternatives
- Information

#6 Verbal & Non-Verbal Communication

Verbal communication is done through intentional and unintentional **phrasing.**

Verbal communication can be transmitted through both spoken and written words.

#6 Verbal & Non-Verbal Communication

Nonverbal communication is done through intentional and unintentional **actions.**

Nonverbal communication refers to signals transmitted through facial expressions, posture, eye contact, gestures, tone of voice, body language, and other ways.

#6 Verbal & Non-Verbal Communication

Be mindful of your unintentional phrasing and actions.

Breakout Assignment:

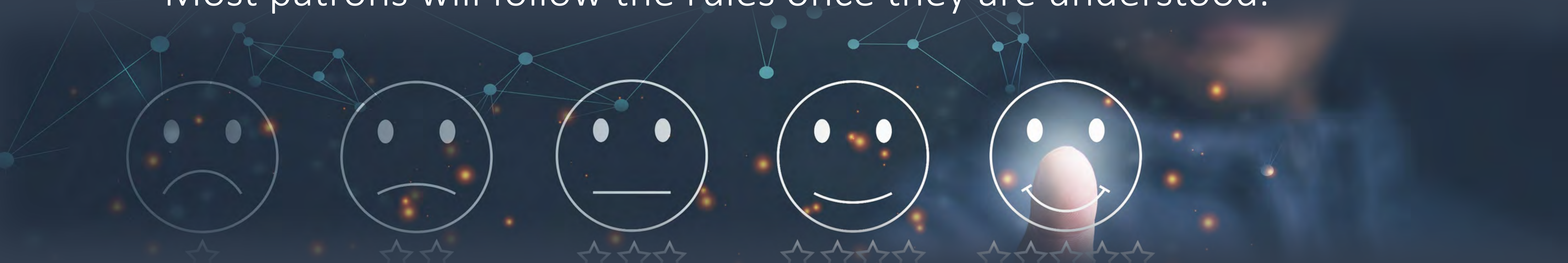
Let’s share some stories in which unintentional actions lead to some disastrous outcomes? And how could they have been prevented?

#7 Handling Enforcement

Why approach: Staff needs to be trained to know the rules and why they need to be enforced.

Patrons are more receptive to comply with a rule if you take the educational approach.

Most patrons will follow the rules once they are understood.



#7 Handling Enforcement

Enforcement should always be firm with fairness and courtesy.

Enforcement should be appropriate for the age of the patron.

#7 Handling Enforcement

Warnings should be given in a professional manner ending in "please" and "thank you".

Refer patrons to a Supervisor, signage or documentation to increase understanding of rules.

#8 Respond… Don’t React

Reactions are personal…do not take things personally!!!

Always respond and don’t react.

Professionals act professionally whether they feel like it or not.

#8 Respond… Don’t React

How to Respond:

The main thing to learn is mindfulness and the pause.

Mindfulness means watching ourselves when something happens that might normally upset us or trigger some sort of emotional reaction.

Pay close attention to how our minds react.

#8 Respond… Don’t React

The Pause:

We don’t have to act immediately…we can pause, not act, breathe.

Sometimes that takes a few seconds, other times it means we should remove ourselves politely from the situation and let ourselves cool down before we respond.

#9 Take the LEAD

When dealing with an angry guest or customer always take the LEAD!

#9 Take the LEAD

Listen

Empathize

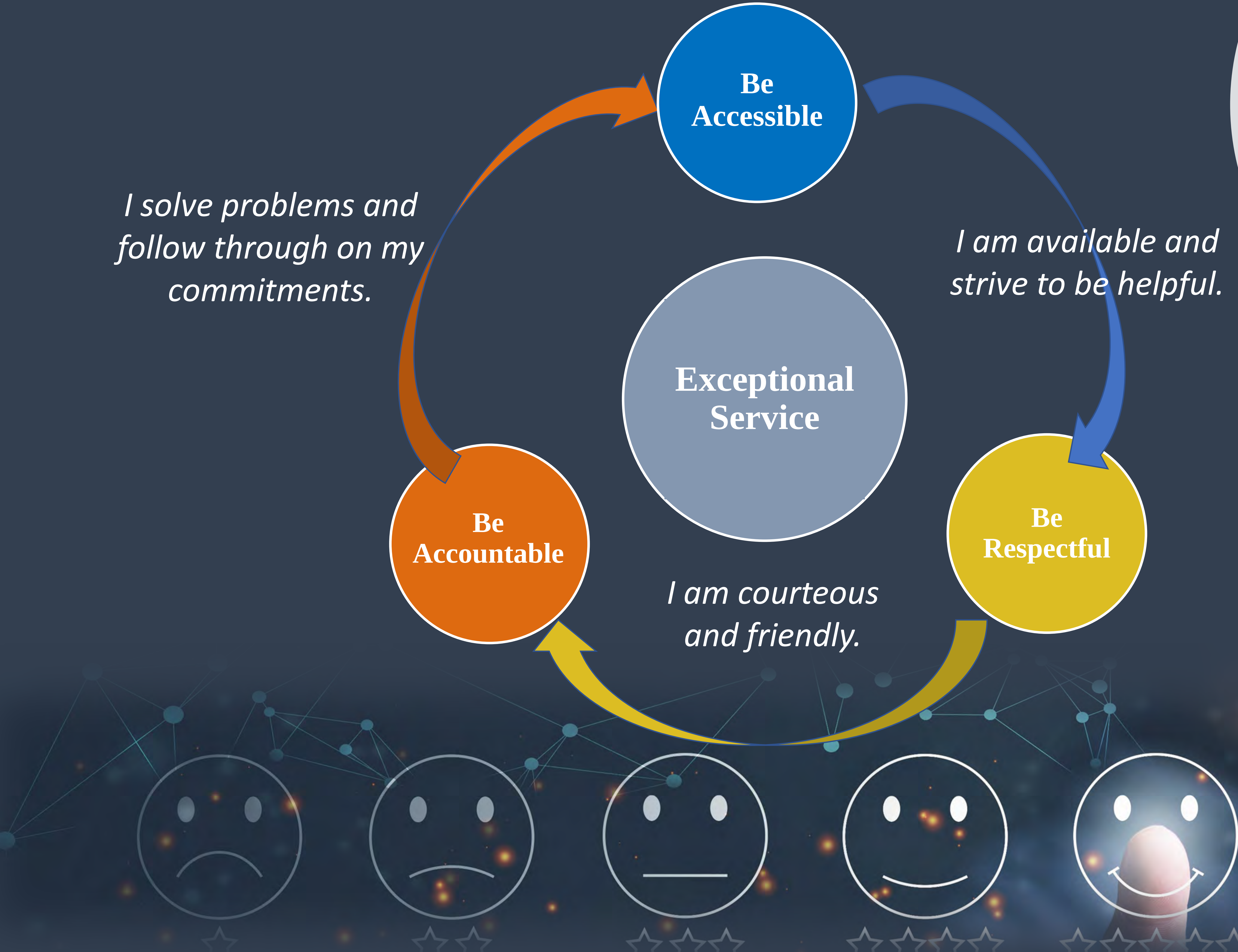
Apologize

Do something or Direct to someone who can

#9 Take the LEAD

Let’s run through a customer scenario.

#10 The Exceptional Customer Service Model



Exceptional Service

Be Accessible

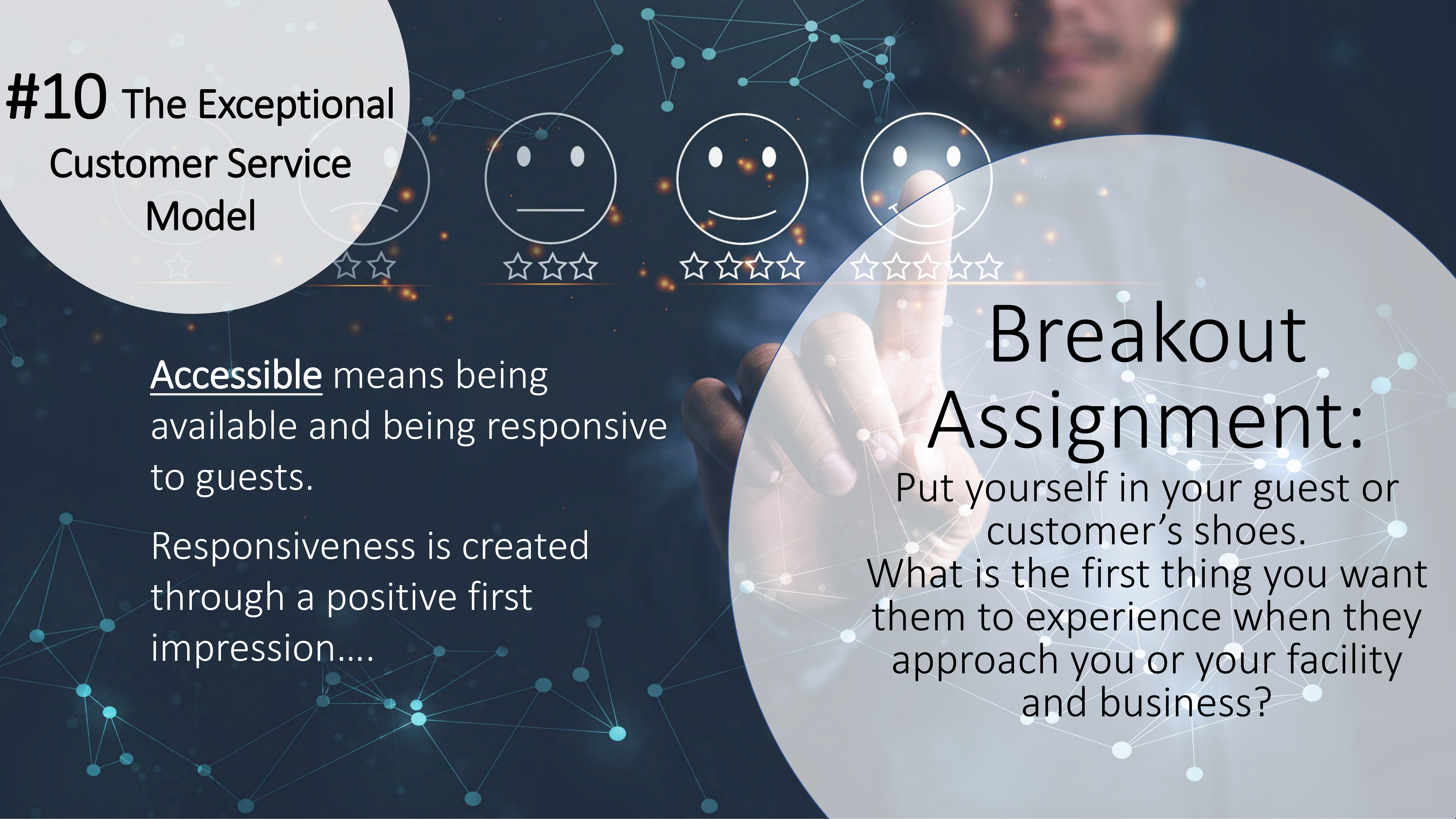
I am available and strive to be helpful.

Be Respectful

I am courteous and friendly.

Be Accountable

I solve problems and follow through on my commitments.



#10 The Exceptional Customer Service Model

__Accessible__ means being available and being responsive to guests.

Responsiveness is created through a positive first impression….

Breakout Assignment:

Put yourself in your guest or customer’s shoes.
What is the first thing you want them to experience when they approach you or your facility and business?

#10 The Exceptional Customer Service Model

<u>Develop your Customer Service Model:</u>
How can you ensure that you have an effective and respectful communications model in your organization?

<u>Respectful</u> means using engaging customer service language that shows respect for our guests.

Tips for Respectful guest communications:

#10 The Exceptional Customer Service Model

Personalize the interaction:

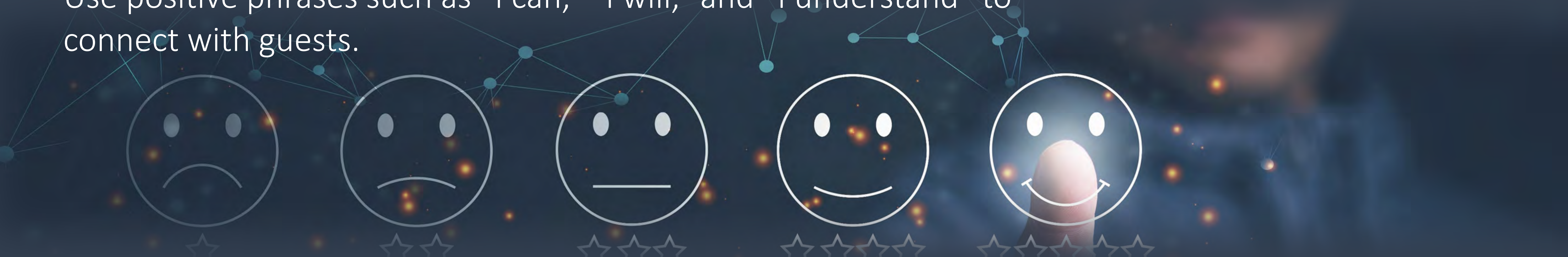
Personalize the experience right from the start. It’s important to introduce yourself and address the customer by name.

Avoid negative phrases:

Avoid words such as “can’t” or “don’t”. Offer to find the solution with determined, positive language.

Use positive language with a touch of empathy:

Use positive phrases such as “I can,” “I will,” and “I understand” to connect with guests.



#10 The Exceptional Customer Service Model

Tips for Respectful guest communications:

Listen closely and avoid interrupting the guest:

Always welcome guests to explain their issues in full before providing solutions. Don’t Interrupt: Interrupting a guest implies a lack of respect or empathy for a problem.

Make communication clear and concise:

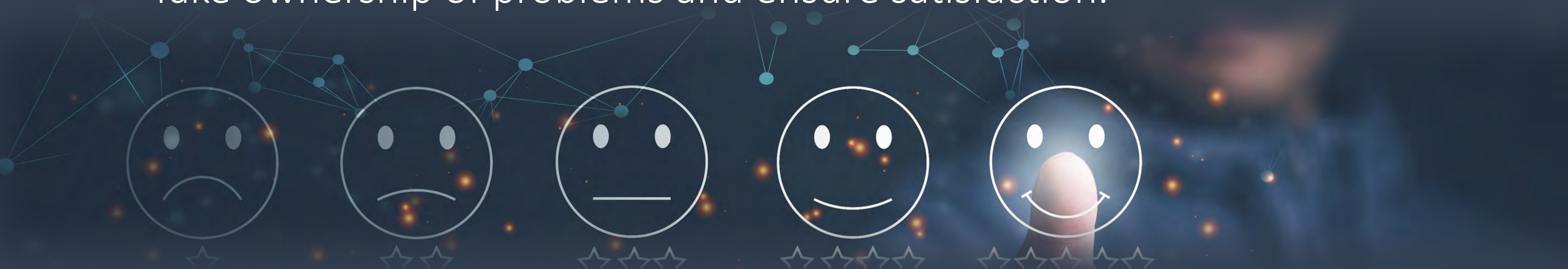
Guests want thorough answers, but they also value their time. Therefore we need to remember that one aspect of effective customer service communication is keeping the exchange fairly concise and always relevant, whether it is verbal or written.

#10 The Exceptional Customer Service Model

What opportunities do you have for demonstrating accountability?

Accountable means quickly solving problems and providing accurate information to the guests.

Take ownership of problems and ensure satisfaction.



How to take ownership…

#10 The Exceptional Customer Service Model

Follow-up within a specific time frame:

Tell the guest what to expect and ensure that they perceive it as responsive.

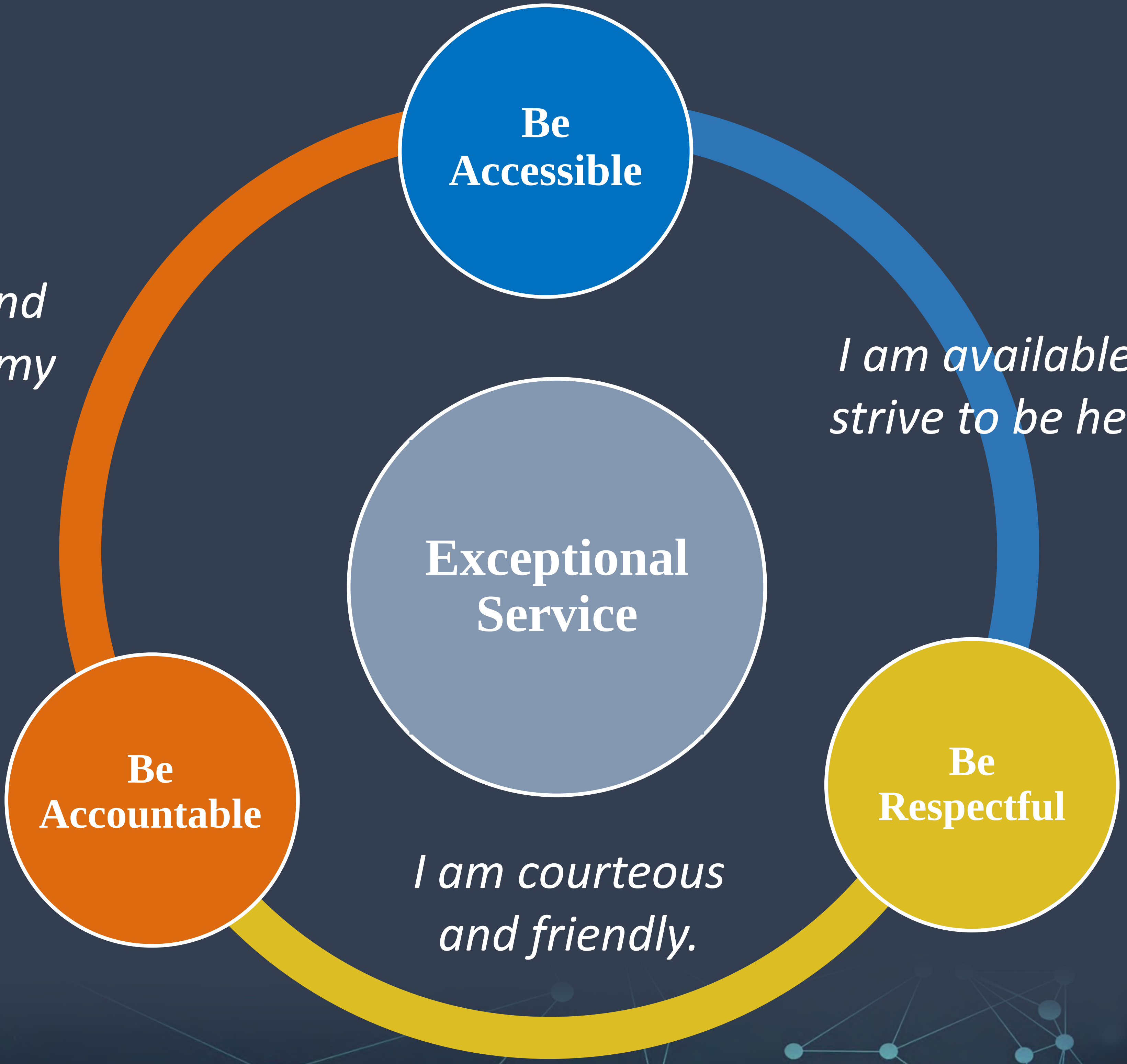
Delays explained before guest has to ask:

Don't wait for the guest to inquire about timing, reach out and let them know about any delays in the process.

Sundown Rule:

Before the sun sets, problems/issues will be cleared up, emails and phone calls returned.

#10 The Exceptional Customer Service Model



Exceptional Service

Be Accessible

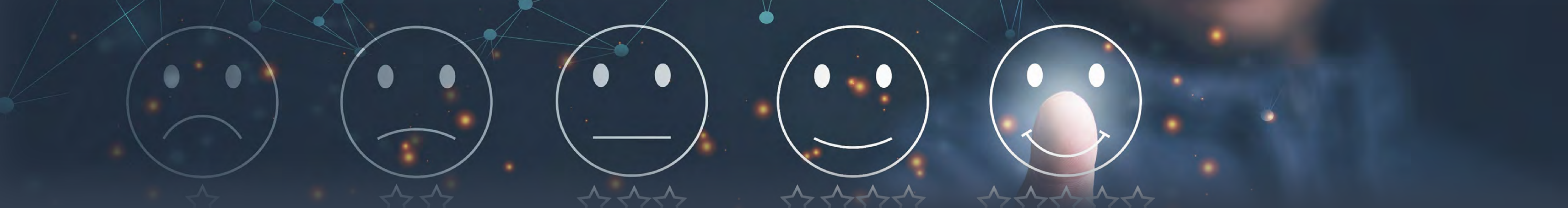
I am available and strive to be helpful.

Be Respectful

I am courteous and friendly.

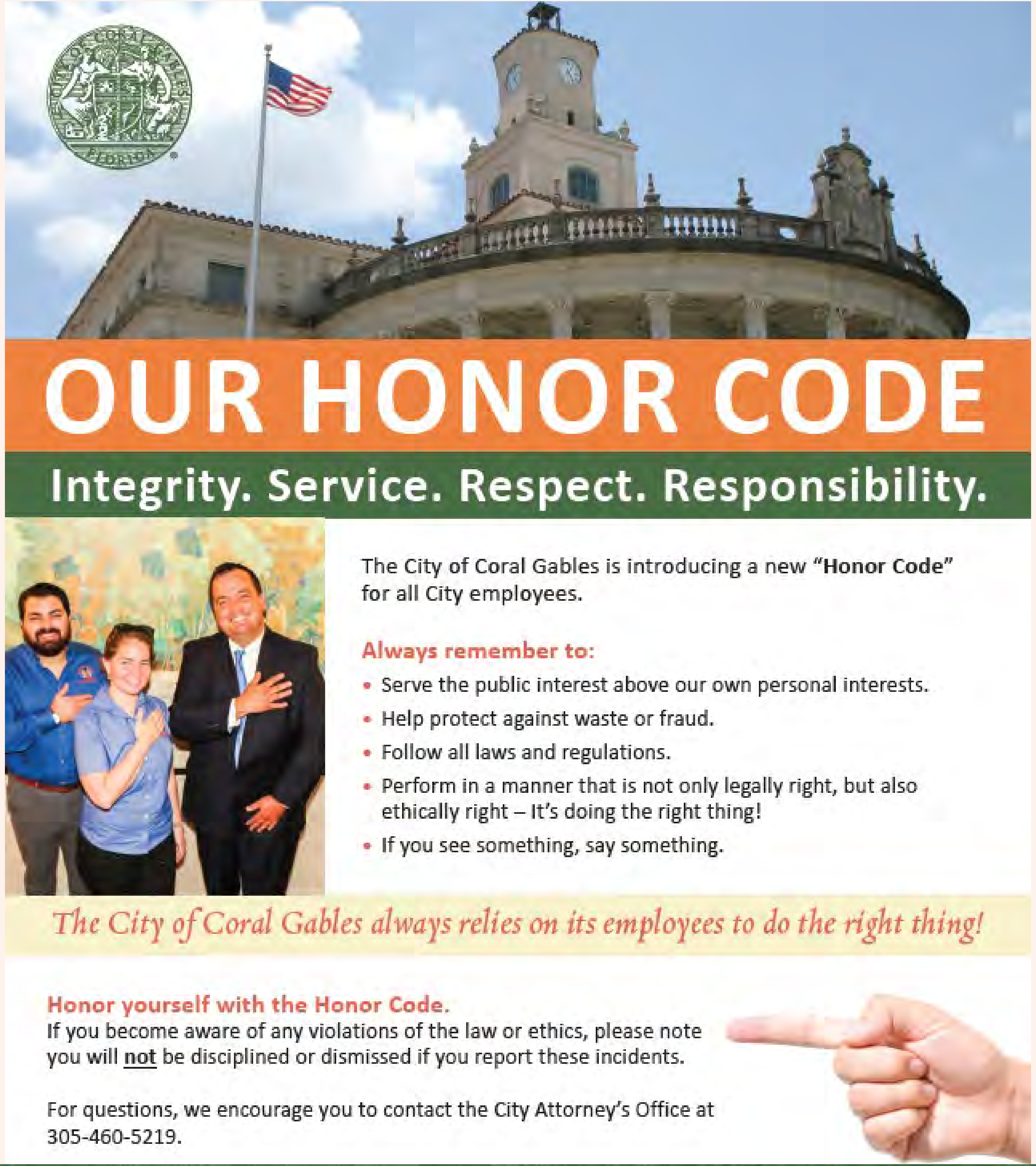
Be Accountable

I solve problems and follow through on my commitments.



Work Environment & Ethics:

- Sexual Harassment Training
  - Leave the locker room talk at home
  - How to handle sexual harassment in the workplace:
    - Identify unwanted behavior
    - Report to a Supervisor
    - Report to Human Resources
- Gift Policy
    - Gifts with monetary value cannot be accepted at any time
    - Alternate options: thank you letter/card or baked goods for the team/office



OUR HONOR CODE

Integrity. Service. Respect. Responsibility.

The City of Coral Gables is introducing a new "**Honor Code**" for all City employees.

Always remember to:

- Serve the public interest above our own personal interests.
- Help protect against waste or fraud.
- Follow all laws and regulations.
- Perform in a manner that is not only legally right, but also ethically right – It's doing the right thing!
- If you see something, say something.

The City of Coral Gables always relies on its employees to do the right thing!

Honor yourself with the Honor Code.
If you become aware of any violations of the law or ethics, please note you will not be disciplined or dismissed if you report these incidents.

For questions, we encourage you to contact the City Attorney's Office at 305-460-5219.

Announcements
Annual Picture
Q&A

The End

CITY OF CORAL GABLES
FLORIDA