Information Technology Policy

City of Coral Gables

Information Technology Department

May 2013

Approved as to form and legal sufficiency

Bridgette Thomton Richard
Deputy City Attorney

IT DEPARTMENT
CHECKED FOR TECHNICAL
COMPLIANCE

Name

Initial Date 5/14/13

RR 5/14/13

5/15/2013

Apprvd:Human Resources Department

Review and approved

Diana M. Gomez
Finance Director

Table of Contents

Introduction

This document serves as the Information Technology Policy for the City of Coral Gables. The purpose of this policy is to ensure the integrity and the protection of Information Resources (defined below) in accordance with local government, state and federal laws and City's rules and regulations. This establishes the information security rules and responsibilities to protect City Information Resources from misuse and/or abuse.

Definitions

1. **Information Resources:**
   Information resources include but are not limited to the following:
   - All City computer hardware, software, telecommunications electronics, networking equipment, internal and external storage devices, and all information-related peripheral components.
   - All electronic multimedia content (data, voice, video, images, etc.) that may be stored in and/or transmitted over any city information resources.
   - All hardcopy documents (paper reports, memos, emails, microfilm, microfiche, films, or any other physical media) containing information, data or proprietary/intellectual property.
   - All computer hardware, software, networking equipment, peripheral components and other electronics connected to any of the City's information resources.
   - Proprietary or sensitive information trusted to the Users such as system passwords and protected records.

2. **City:**
   City of Coral Gables.

3. **IT:**
   Information Technology.

4. **Stakeholder:**
   An individual department director who has primary responsibility for the particular data/information within an Information Resource IT system.

5. **User(s):**
   Anyone using the City's Information Resources.

Applicability

This policy applies to all City staff and Users and anyone who has access to and/or uses any City Information Resources.

Roles and Responsibilities

All City staff and Users share the responsibility of protecting the Information Resources for which they have access and/or ownership.

Information Technology Policy Steering Committee

The Information Technology Policy Steering Committee consists of departmental directors with Stakeholder and/or IT responsibilities and has the following responsibilities:

1. Provide the leadership to establish a secure and reliable infrastructure to protect the City's Information Resources.

2. Develop and maintain an IT policy with the coordination of appropriate Information Resources Stakeholders.

IT Security Team

The IT Security Team is responsible for implementing the City's IT policy to include the following:

1. Implement, secure and monitor Information Resources activities for IT policy compliance and best practices.

2. Monitor and block or remove from the City's network any Information Resource that violates this policy and take necessary actions to protect and prevent potential damages to City's Information Resources.

3. Investigate all actual or potential information security incidents or violations of this policy and document their findings.

4. Work with the Human Resources (HR) Department to develop information security education and training for all City employees.

5. The IT Security Team with the advice and consent of the CIO may permit deviations from this policy if such deviations are required to maintain continuity of Information Resources operation for the City.

Stakeholders

Stakeholders are department directors with primary responsibility for particular data/information systems. They determine who is authorized to access City Information Resources under their management. They shall make sure that those with access have a need to know the information and know the security requirements for that information. Information may be disclosed only if disclosure is consistent with law, regulations and City policies. Stakeholders shall work with the IT Department to keep records

documenting the creation, distribution, and disposal of City information. Stakeholders shall report suspected or known compromises of their information to the IT Security Team at ITSecurity@coralgables.com, HR Department, and/or the appropriate law enforcement authority when required.

Users

Users must protect the Information Resources they have access to or that they control (i.e., passwords, computers, and data.) Users must also adhere to all City Information Technology policies and procedures.

Information Classification

Data and information that are owned by the City must be protected in accordance with City's rules and regulations, local government, state and federal laws. The Information Technology Policy Steering Committee is responsible for developing, monitoring and maintaining these classifications.

Policy Violations

It is a violation of this policy to:

1. Interfere with the normal operation of any City Information Resources.

2. Use City Information Resources to interfere with the normal operation of other information resources outside of the City.

3. Use City Information Resources to:
   a) Violate local, state, federal or international law
   b) Cause, encourage or facilitate others in violating local, state, federal or international law

4. Access or cause another to access any Information Resources without permission of the City or the appropriate Stakeholders.

5. Access or cause another to access intellectual property, copyright-protected property or other legally protected property without permission from the property's owner.

6. Release information resources without the approval of the appropriate City department.

7. Use any Information Resources to violate any policy of the City.

8. Use any Information Resources to violate the IT policy and/or other operational policies of organizations or institutions outside of the City.

9. To intentionally use and/or transmit software, data files or other materials that can be reasonably considered as computer viruses, Trojans or other "malware."

10. Scan and/or copy any City Information Resources without written approval of the Stakeholders.

11. Capture or monitor network transmissions, telecommunications transmissions, or any information resources without written approval of the IT Security Team or, in the case of data, written permission of the appropriate Stakeholders.

12. Share user IDs, passwords, identity cards or other means of access to Information Resources.

13. Connect or disconnect any device to an information resource without written permission of the IT Security Team. General exceptions are given to IT staff that, as part of their normally assigned duties, continually connect and disconnect equipment from information resources. In addition, a general exception is given to connect storage devices to City Information Resources if:

    a) The person connecting the device is authorized to use the information resource they are connecting to.
    b) The device does not interfere with the normal operation of Information Resources.
    c) Connecting this device does not otherwise violate this policy.

14. Install or connect to any City Information Resources, telecommunications equipment and/or networking components without the written permission of the appropriate Stakeholders. General exceptions are given to IT staff that, as part of their normally assigned duties, install or connect telecommunications and networking equipment.

Rights Reserved

The City reserves the rights to:

1. Examine or monitor any Information Resource including, but not limited to, equipment, software, computer files, information and data. The following is a list of situations where the City may invoke this right. This is not intended as an exhaustive list.

    - Required by legal authority.
    - The information resource in question may be in violation of City rules and regulations.
    - The IT Department deems it necessary for the efficient and effective operation of the City's Information Resources.
    - The IT Department is directed to do so by the City Manager's Office, Human Resources Department, Police Department and/or City Attorney's office.
    - It is required for IT staff to perform repair or normal operation and maintenance activity.
    - Reasons determined by the Information Technology Policy Steering Committee.

2. Remove or block User access to any City Information Resources at any time when any of the following conditions exist:

- A user violates any City policies.
- A user interferes with the operation of City Information Resources.
- A user violates any city, state and/or federal law or regulation.
- For other reasons as determined by the Information Technology Policy Steering Committee and approved by the CIO.

3. Report to local, state or federal authorities regarding Information Resources related activities that appear to violate the law or a regulation.

Reporting Violations

All City Information Resources Users will report violations or suspected violations of this policy to the IT Security Team at ITSecurity@coralgables.com. Alternatively, violations or suspected violations may be reported to the HR Department or to law enforcement when appropriate. IT staff, which become aware of a potential or suspected violation of this policy through the normal course of their work, are required to inform the CIO of the event.

Policy Violation Disciplines and Prosecutions

Anyone found to have violated this policy will be disciplined per the City's rules and regulations, and may be prosecuted in accordance with local, state and/or federal laws where applicable.