Information Security Policy

Effective January 1, 2009

CFMC Information Security Policy

Effective January 1, 2009

Introduction

Computer information systems and networks are an integral part of our business. The Community Foundation for Monterey County (CFMC) has made a substantial investment in human and financial resources to create these systems.

The enclosed policies and directives have been established in order to:

1. Establish a Foundation-wide approach to information security.
2. Protect our investment.
3. Safeguard the information contained within these systems.
4. Reduce business and legal risk.
5. Protect the reputation of the Foundation as well as protect the Foundation of its legal and ethical responsibilities.

General Policy

CFMC uses a layered approach of overlapping controls, monitoring and authentication to ensure overall security of the Foundation's data, network and system resources. It is CFMC policy to take all reasonable measures to protect the confidentiality, integrity, and availability of its information and information systems. CFMC will ensure full compliance with all applicable state and federal statutes and regulations.

Security reviews of servers, firewalls, routers and monitoring platforms must be conducted on a regular basis. These reviews must include monitoring access logs and results of intrusion detection software, where it has been installed.

Violations

Violations may result in disciplinary action in accordance with Foundation policy. Failure to observe these guidelines may result in disciplinary action depending upon the type and severity of the violation, whether it causes any liability or loss to the Foundation, and/or the presence of any repeated violation(s).

Administration

The Administrative Services Manager (ASM) is responsible for the administration of this policy. From time to time the ASM may delegate or assign responsibility for basic day to day administration of the policy.

Contents

The topics covered in this document include:

1. Statement of Responsibility

General responsibilities pertaining to this policy are set forth in this section. The following sections list additional specific responsibilities.

A. Manager Responsibilities

Managers and supervisors must:

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

B. Information Technology responsibilities

The Information Technology (IT) department must:

- Develop and maintain written standards and procedures necessary to ensure implementation of and compliance with these policy directives.
- Provide appropriate support and guidance to assist employees to fulfill their responsibilities under this directive.

2. The Internet and Email

The Internet is a very large, publicly accessible network that has millions of connected users and organizations worldwide. One popular feature of the Internet is email.

• Policy

Access to the Internet is provided to employees for the benefit of CFMC and its constituents. Employees are able to connect to a variety of business information resources around the world.

Conversely, the Internet is also replete with risks and inappropriate material. To ensure that all employees are responsible and productive Internet users and to protect the Foundation's interests, the following guidelines have been established for using the Internet and email.

• Acceptable use

Employees using the Internet are representing the organization. Employees are responsible for ensuring that the Internet is used in an effective, ethical, and lawful manner. Examples of acceptable use are:

- Using Web browsers to obtain business information from official Web sites.
- Accessing databases for information as needed.
- Using email for business contacts.
- For email groups of more than 40 the use of Constant Contact third party email marketing service must be used to manage the large amount of data.

Unacceptable use
Employees must not use the Internet for purposes that are illegal, unethical, harmful to the organization, or nonproductive. Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.

- Broadcasting email, i.e., sending the same message to more than 40 recipients or more than one distribution list.
- Conducting a personal business using Foundation resources.
- Transmitting any content that is offensive, harassing, or fraudulent.

- **Downloads**

  File downloads from the Internet are not permitted unless specifically authorized in writing by the IT department. Some examples of unacceptable products are: Google Toolbar, music, commercial entertainment or any services not work related.

- **Employee responsibilities**

  An employee who uses the Internet or Internet e-mail shall:

  1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
  2. Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet. All communications should have the employee's name attached.
  3. Not transmit copyrighted materials without permission.
  4. Know and abide by all applicable organizational policies dealing with security and confidentiality of organization records.
  5. Allow a virus scan on any executable file(s) received through the Internet.
  6. Avoid transmission of nonpublic customer information. If it is necessary to transmit nonpublic information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorized to receive such information for a legitimate use.

- **Copyrights**

  Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner. Failure to observe copyright or license agreements may result in disciplinary action by the organization and/or legal action by the copyright owner.

- **Monitoring**

  All messages created, sent, or retrieved over the Internet are the property of the Foundation and *may be regarded as public information*. CFMC reserves the right to access the contents of any messages sent over its facilities if the organization believes, in its sole judgment, that it has a business need to do so.

  NOTE:

  All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. **This means don't put anything into your email messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.**

3. Computer Viruses

Computer viruses are programs designed to make unauthorized changes to programs and data. Therefore, viruses can cause destruction of corporate resources.

A. Background

It is important to know that:

- Computer viruses are much easier to prevent than to cure.
- Defenses against computer viruses include protection against unauthorized access to computer systems, using only trusted sources for data and programs, and maintaining virus-scanning software.

B. IT Responsibilities

IT shall:

1. Install and maintain appropriate antivirus software on all computers.
2. Respond to all virus attacks, destroy any virus detected, and document each incident.

C. Employee Responsibilities

These directives apply to all employees:

1. Employees shall not knowingly introduce a computer virus into organization computers.
2. Employees shall not load diskettes, compact disks (CDs) or USB memory sticks of unknown origin.
3. Incoming diskettes, CDs and USB memory sticks shall be scanned for viruses before they are read.
4. Any associate who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY POWER OFF the workstation and call the IT or his/her manager.

4. Access Codes and Passwords

The confidentiality and integrity of data stored on organization computer systems must be protected by access controls to ensure that only authorized employees have access. This access shall be restricted to only those capabilities that are appropriate to each employee's job duties.

A. IT Responsibilities

The IT department shall be responsible for the administration of access controls to all organization computer systems. The IT department will process adds, deletions, and changes upon receipt of a written request from the end user's supervisor.

Deletions may be processed by an oral request prior to reception of the written request. The IT department will maintain a list of administrative access codes and passwords and keep this list in a secure area.

Automated network policies will be enabled to enforce the following policies:

1. Request password changes no less than every six months.
2. Passwords at least eight characters long;
3. Retain password history of at least three previous passwords;
4. Require complex passwords. (At least one upper case letter, one lower case letter and one number.);
5. Automatically lock a computer after 15 minutes of idle time and require a password to log back in.

B. Employee Responsibilities

Each employee:

1. Shall be responsible for all computer transactions that are made with his/her User ID and password.
2. Shall not disclose passwords to others. Passwords must be changed immediately if it is suspected that they may have become known to others. Passwords should not be recorded where they may be easily obtained.
3. Will change passwords at least every 180 days. (IT may force password changes when required.)
4. Should use passwords that will not be easily guessed by others.
5. Should log out when leaving a workstation for an extended period.

C. Supervisor's Responsibility

Managers and supervisors should notify the IT manager promptly whenever an employee leaves the organization or transfers to another department so that his/her access can be revoked. Involuntary terminations must be reported concurrent with the termination.

D. Human Resources Responsibility

The Personnel Department will notify IT monthly of associate transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

5. Physical Security

It is Foundation policy to protect computer hardware, software, data, and documentation from misuse, theft, unauthorized access, and environmental hazards.

A. Employee Responsibilities

The directives below apply to all employees:

1. USB memory sticks will be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be labeled appropriately and locked up when not in use.
2. Diskettes, CDs and USB memory sticks should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields (cell phones and microwaves.)
3. Critical computer equipment, e.g., file servers, must be protected by an uninterruptible power supply (UPS). Other computer equipment should be protected by a surge suppressor at a minimum.
4. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
5. Since the IT department is responsible for all equipment installations, disconnections, modifications, and relocations, employees are not to perform these activities unless granted permission in advance. This does not apply to temporary moves of portable computers for which an initial connection has been set up by IT.
6. Employees shall not remove shared portable equipment such as laptop computers without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.

7. Employees should exercise care to safeguard the valuable electronic equipment assigned to them. Employees who neglect this duty may be accountable for any loss or damage that may result.

6. Copyrights and license agreements

It is Foundation policy to comply with all laws regarding intellectual property.

A. Legal Reference

CFMC and its employees are legally bound to comply with the Federal Copyright Act (Title 17 of the U. S. Code) and all proprietary software license agreements. Noncompliance can expose the organization and the responsible employee(s) to civil and/or criminal penalties.

B. Scope

This directive applies to all software that is owned by CFMC, licensed to CFMC, or developed using CFMC resources by employees or vendors.

C. IT Responsibilities

The IT department will:

1. Maintain records of software licenses owned by the organization.
2. Periodically (at least annually) scan organization computers to verify that only authorized software is installed.

D. Employee Responsibilities

Employees shall not:

1. Install software unless authorized by IT. Only software that is licensed to or owned by the organization is to be installed on the organization's computers.
2. Copy software unless authorized by IT.
3. Download software unless authorized by IT.

E. Civil Penalties

Violations of copyright law expose the organization and the responsible employee(s) to the following civil penalties:

- Liability for damages suffered by the copyright owner
- Profits that are attributable to the copying
- Fines up to $100,000 for each illegal copy

F. Criminal Penalties

Violations of copyright law that are committed "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))," expose the organization and the employee(s) responsible to the following criminal penalties:

- Fines up to $250,000 for each illegal copy
- Jail terms of up to five years

Acknowledgment of Information Security Policy

This form is used to acknowledge receipt of, and compliance with, the CFMC Information Security Policy.

Procedure

Complete the following steps:

1. Read the Information Security Policy.
2. Sign and date in the spaces provided below.
3. Return this page only to the Director of Finance and Human Resources.

Signature

By signing below, I agree to the following terms:

i. I have received and read a copy of the "Information Security Policy" and understand the same;
ii. I understand and agree that any computers, software, and storage media provided to me by the organization contains proprietary and confidential information about CFMC and its constituents or its vendors, and that this is and remains the property of the Foundation at all times;
iii. I agree that I shall not copy, duplicate (except for backup purposes as part of my job here at CFMC), otherwise disclose, or allow anyone else to copy or duplicate any of this information or software;
iv. I agree that, if I leave CFMC for any reason, I shall immediately return to the Foundation the original and copies of any and all software, computer materials, or computer equipment that I may have received from the organization that is either in my possession or otherwise directly or indirectly under my control.

Employee signature: _____

Employee name: _____

Date: _____

Department: _____