California State University, Fresno Association Inc.
Information Security and Hardware/Software Policy

Table of Contents

California State University, Fresno Association Inc.
Information Security and Hardware/Software Policy

(The following policy supersedes and replaces all references in the Employee Hand Book)

Information Security and Hardware/Software Policy

Computer information systems and networks are an integral part of business of the California State University, Fresno Association Inc. ("the Association"). The Association 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 protect this investment, safeguard the information contained within these systems, reduce business and legal risk, and protect the good name of the company.

Acceptable use

This section defines what constitutes "acceptable use" of the company's electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the company are to be used only for creating, researching, and processing company-related materials, and other tasks necessary for performing one's employment duties. By using the company's hardware, software, and network systems you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable company policies, as well as city, state, and federal laws and regulations.

Violations

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

Administration

The MIS director is responsible for the administration of this policy. This policy is a living document and may be modified at any time by the MIS Director or the Association Executive Director.

Director and Supervisor Responsibilities

- Ensure that all appropriate personnel are aware of and comply with this policy.
- Implement and support this policy within their respective departments, as well as create practices/procedures (specific to their departments) that are designed to provide reasonable assurance that all employees observe this policy.

MIS Director Responsibilities

- Develop and maintain written 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.

The Internet and e-mail

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 e-mail.

Access to the Internet is provided to employees for the benefit of the Association and its employees. Employees are able to connect to a variety of 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 company's interests, the following guidelines have been established for using the Internet and e-mail.

Acceptable use

Employees using the Internet are representing the company. Employees are responsible for ensuring that the Internet is used in a safe, effective, ethical, and lawful manner and only in the course of performing the employees' job.

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

- Ensure that all communications are for work-related reasons and that they do not interfere with his/her productivity.
- Be responsible for the content of all text, audio, or images that (s)he places or sends over the Internet, and not illegally transmit or receive the same. All communications should have the employee's name attached.
- Not transmit copyrighted materials without permission.
- Know and abide by all applicable policies dealing with security and confidentiality of records.
- Run a virus scan on any external files received on flash drive or CD's.

Unacceptable use

Employees must only use the Internet for purposes that are company-related. Content that is illegal, unethical, inappropriate for a University setting, harmful to the University or the company, or nonproductive are prohibited.

Examples of unacceptable use are:

- Sending or forwarding chain e-mail, i.e., messages containing instructions to forward the message to others.
- Broadcasting e-mail, i.e., sending the same message to more than 10 recipients or more than one distribution list.
- Conducting a personal business using company resources.
- Transmitting any content that is offensive, harassing, or fraudulent.
- Participating in Internet "chat" rooms.
- Downloading or storing of music files anywhere on the network – including your 'personal' directories or your local 'C' drive.

Downloads

File downloads from the Internet are **NOT** permitted unless specifically authorized in writing by the MIS director.

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 company and/or legal action by the copyright owner. In addition, illegal file sharing is a violation of Title 5 of the California Code of Regulations and may also result in disciplinary action.

Monitoring

All messages created, sent, or retrieved over the Internet are the property of the company and *may be regarded as public information*. The Association reserves the right to access the contents of any messages sent over its facilities or using its equipment, if the company believes, in its sole discretion, that it has a business reason to do so.

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. **Do not put anything in your e-mail messages that you wouldn't want to see on the front page of the newspaper or be able to explain to your employer.**

Computer Viruses

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

MIS will install and maintain appropriate antivirus software on all computers and will respond to all virus attacks. All virus related incidents will be documented.

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.

The following applies to all employees:

- Employees shall not knowingly introduce a computer virus into company computers.
- Employees shall only load CD's, DVD's or Flash Drives with saved files that pertain to company business.
- Incoming CD's, DVD's or Flash Drives shall be scanned for viruses before they are read.
- Any employee who suspects that his/her workstation has been infected by a virus shall IMMEDIATELY log off the network and call the MIS help desk at 8-0820.
- Users shall not disable the automated Anti-Virus Download Scan.

Access Codes and Passwords

The confidentiality and integrity of data stored on company 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.

The MIS director shall be responsible for the administration of access controls to all company computer systems. The MIS director will ensure the process of 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.

MIS Responsibilities

- Ensure contractors credentials have restricted hours whenever possible. Disable contractor credentials when project is complete and/or not active.
- Do periodic audits against user logon and logoff, looking for things out of the ordinary, such as logons after normal business, excessive lockouts, etc.
- The MIS director will maintain a list of administrator and/or security officer access codes and passwords and keep this list in the MIS safe.

Employee responsibilities

Network logon is the first line of defense for company network resources. This section is intended to establish responsibilities to protect the network's front door. Being lax about network logon and passwords is like giving strangers the key to your home's front door. Because your logon allows you entrance to the network's front door, employees must take every precaution to protect their logon information.

Each employee:

- Shall be responsible for all computer transactions that are made with his/her User ID and password.
- Shall NOT disclose or share their password with others. Passwords must be changed immediately if it is suspected others may know it. Direct password change requests to the MIS help desk.
  - Passwords shall not be recorded or stored where they may be easily obtained.
  - Passwords shall **NOT** be stored on shared drives or the local 'C' drive. Appropriate places to store passwords are in a wallet, safe, locked cabinet or drawer that is not shared with other employees.
  - Passwords should **NEVER** be communicated over the Internet and/or email.
- Should use passwords that will not be easily guessed by others; values such as names of any kind, birthday or social security number, current month, sports teams, etc. are NOT acceptable passwords.
- Will be prompted to change passwords at least every 90 days. The exception to this is 'Inquiry users' such as Project Directors. These users have inquiry access only and will NOT be required to change passwords. However, they are encouraged to change their password when they feel it has been compromised and/or when staff changes within their department.
- Should lock computers at all times when away from their desks by using the *Windows Lock Computer* function. Call the Auxiliary MIS help desk for assistance with this function if needed.

Supervisor's responsibility

Directors and supervisors should notify the MIS director promptly whenever an employee leaves the company or transfers to another department so that his/her access can be revoked and/or changed as necessary. Involuntary terminations must be reported concurrent with the termination.

Human Resources responsibility

The Human Resources Department will notify MIS immediately of employee transfers and terminations. Involuntary terminations must be reported concurrent with the termination.

Hardware

All hardware devices acquired by the Association or developed by it (through its own employees or through those hired by the Association to develop the hardware devices) is and at all times shall remain company property. All such hardware devices must be used in compliance with applicable licenses, notices, contracts, and agreements.

Purchasing

All purchasing of company computer hardware devices shall be centralized within the MIS department to ensure that all equipment conforms to corporate hardware standards and is purchased or leased at the best possible price.

All requests for corporate computing hardware devices must be in the annual corporate budget document and have the department Directors approval. The request must then be sent to the MIS department, who will review the need for such hardware, and then determine standard hardware that best accommodates the desired request, if MIS determines that such hardware is needed.

Hardware standards

Hardware configurations are reviewed with each new lease in order to determine what equipment will best meet the needs of the end user. The MIS department makes every effort to provide the most suitable desktop or laptop while maintaining company cost effectiveness.

Employees will be given access to appropriate network printers. In some limited cases, employees may be given local printers if deemed necessary by the department director in consultation with the MIS department.

Employees needing computer hardware beyond that which is typically provided must request such hardware from the MIS department. Each request will be considered on a case-by-case basis in conjunction with the hardware-purchasing section of this policy.

Outside equipment

No outside equipment may be connected to the company's network without the MIS department's written permission.

Software

All software acquired for or on behalf of the company or developed by company employees or contract personnel on behalf of the company is and at all times shall remain company property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

Purchasing

All purchasing of company software shall be centralized within the MIS department to ensure that all applications conform to corporate software standards and are purchased at the best possible price. All requests for corporate software must be submitted to the department Director for his/her approval. The request must then be sent to the MIS department, which will review the need for such software, and then determine the standard software that best accommodates the desired request, if MIS determines that such software is needed.

Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on company computers. If an employee needs help in interpreting the meaning/application of any such licenses, notices, contracts and agreements, he/she will contact MIS for assistance. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of the company's Hardware/Software Policy.

Software Standards

The Management Information Systems department will install and configure a standard package of software on company computers that will best enable users to perform their daily duties. Employees needing software beyond that which is provided must request such software from the MIS department. Each request will considered on a case by case basis in conjunction with the software purchasing section of this policy.

Software Installation

The MIS department is exclusively responsible for installing and supporting all software on company computers and telecommuter home computers that are provided by the company.

California State University, Fresno Association Inc.
Information Security and Hardware/Software Policy

Acknowledgment of Information Security and Hardware/Software Policy

This form is used to acknowledge receipt of and pledge compliance with the Association's Information Security and Hardware/Software Policy.

Complete the following steps:

1. Read the Information Security and Hardware/Software Policy.
2. Initial the spaces provided below, Sign and date the last page.
3. Return to the Management Information Services Director.

Initial

By initialing below, I agree to the following terms:

(i) I have received and read a copy of the Information Security and Hardware/Software Policy and understand and agree to abide by the same.

(ii) I understand and agree that any hardware and software provided to me by the company remain the property of the company.

(iii) I understand and agree that I am not to modify, alter, or upgrade any software programs or hardware devices provided to me by the organization without the permission of the MIS Department.

(iv) I understand and agree that I shall not copy, duplicate (except for backup purposes as part of my job), or allow anyone else to copy or duplicate any software.

(v) I agree that if I leave the employment of the California State University, Fresno Association, Inc. for any reason, I shall immediately return to the company the original and copies of any and all software, computer materials, or computer equipment that I may have received from the Association that is either in my possession or otherwise directly or indirectly under my control.

(vi) I understand and agree I must make reasonable efforts to protect all Association-provided software and hardware devices from theft and physical damage.

_____ _____

Employee Signature Date

_____ _____

Employee Name Employee Title

_____

Department / Location