Information Technology Use

342.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidelines for the proper use of department information technology resources, including computers, electronic devices, hardware, software and systems.

342.1.1 DEFINITIONS

Definitions related to this policy include:

Computer system - All computers (on-site and portable), electronic devices, hardware, software, and resources owned, leased, rented or licensed by the CSU Police Department, San Luis Obispo that are provided for official use by its members. This includes all access to, and use of, Internet Service Providers (ISP) or other service providers provided by or through the Department or department funding.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, electronic devices, telephones, including cellular and satellite, pagers, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs, systems and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Any electronic document, information or data residing or located, in whole or in part, on the system including, but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports, messages, photographs or videos.

342.2 POLICY

It is the policy of the CSU Police Department, San Luis Obispo that members shall use information technology resources, including computers, software and systems, that are issued or maintained by the Department in a professional manner and in accordance with this policy.

342.3 PRIVACY EXPECTATION

Members forfeit any expectation of privacy with regard to emails, texts, or anything published, shared, transmitted, or maintained through file-sharing software or any internet site that is accessed, transmitted, received, or reviewed on any department computer system.

The Department reserves the right to access, audit, and disclose, for whatever reason, any message, including attachments, and any information accessed, transmitted, received, or reviewed over any technology that is issued or maintained by the Department, including the department email system, computer network, and/or any information placed into storage on any department system or device. This includes records of all keystrokes or Web-browsing history made at any department computer or over any department network. The fact that access to a database, service, or website requires a username or password will not create an expectation of privacy if it is accessed through department computers, electronic devices, or networks.

The Department shall not require a member to disclose a personal username or password for accessing personal social media or to open a personal social website; however, the Department may request access when it is reasonably believed to be relevant to the investigation of allegations of work-related misconduct (Labor Code § 980).

342.4 RESTRICTED USE

Members shall not access computers, devices, software or systems for which they have not received prior authorization or the required training. Members shall immediately report unauthorized access or use of computers, devices, software or systems by another member to their supervisors or Watch Commanders.

Members shall not use another person's access passwords, logon information and other individual security data, protocols and procedures unless directed to do so by a supervisor.

342.4.1 SOFTWARE

Members shall not copy or duplicate any copyrighted or licensed software except for a single copy for backup purposes in accordance with the software company's copyright and license agreement.

To reduce the risk of a computer virus or malicious software, members shall not install any unlicensed or unauthorized software on any department computer. Members shall not install personal copies of any software onto any department computer.

When related to criminal investigations, software program files may be downloaded only with the approval of the information systems technology (IT) staff and with the authorization of the Chief of Police or the authorized designee.

No member shall knowingly make, acquire or use unauthorized copies of computer software that is not licensed to the Department while on department premises, computer systems or electronic devices. Such unauthorized use of software exposes the Department and involved members to severe civil and criminal penalties.

Introduction of software by members should only occur as part of the automated maintenance or update process of department- or University-approved or installed programs by the original manufacturer, producer or developer of the software.

Any other introduction of software requires prior authorization from IT staff and a full scan for malicious attachments.

342.4.2 HARDWARE

Access to technology resources provided by or through the Department shall be strictly limited to department-related activities. Data stored on or available through department computer systems shall only be accessed by authorized members who are engaged in an active investigation or assisting in an active investigation, or who otherwise have a legitimate law enforcement or department-related purpose to access such data. Any exceptions to this policy must be approved by a supervisor.

342.4.3 INTERNET USE

Internet access provided by or through the Department shall be strictly limited to department-related activities. Internet sites containing information that is not appropriate or applicable to department use and which shall not be intentionally accessed include but are not limited to adult forums, pornography, gambling, chat rooms, and similar or related internet sites. Certain exceptions may be permitted with the express approval of a supervisor as a function of a member’s assignment.

Downloaded information shall be limited to messages, mail, and data files.

342.4.4 OFF-DUTY USE

Members shall only use technology resources provided by the Department while on-duty or in conjunction with specific on-call assignments unless specifically authorized by a supervisor. This includes the use of telephones, cell phones, texting, email or any other "off the clock" work-related activities. This also applies to personally owned devices that are used to access department resources.

Refer to the Personal Communication Devices Policy for guidelines regarding off-duty use of personally owned technology.

342.5 PROTECTION OF AGENCY SYSTEMS AND FILES

All members have a duty to protect the computer system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care, and maintenance of the computer system.

Members shall ensure department computers and access terminals are not viewable by persons who are not authorized users. Computers and terminals should be secured, users logged off and password protections enabled whenever the user is not present. Access passwords, logon information, and other individual security data, protocols, and procedures are confidential information and are not to be shared. Password length, format, structure, and content shall meet the prescribed standards required by the computer system or as directed by a supervisor and shall be changed at intervals as directed by IT staff or a supervisor.

It is prohibited for a member to allow an unauthorized user to access the computer system at any time or for any reason. Members shall promptly report any unauthorized access to the computer system or suspected intrusion from outside sources (including the internet) to a supervisor.

342.6 INSPECTION OR REVIEW

A supervisor or the authorized designee has the express authority to inspect or review the computer system, all temporary or permanent files, related electronic systems or devices, and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

Reasons for inspection or review may include, but are not limited to, computer system malfunctions, problems or general computer system failure, a lawsuit against the Department involving one of its members or a member’s duties, an alleged or suspected violation of any department policy, a request for disclosure of data, or a need to perform or provide a service.

The IT staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the department computer system when requested by a supervisor or during the course of regular duties that require such information.

342.7 SYSTEMS ACCESS, PHYSICAL SECURITY, AND RECORDS RETENTION

342.7.1 CLETS EMPLOYEE/VOLUNTEER STATEMENT FORM/DMV INFORMATION SECURITY STATEMENT

Generally, access to and use of information from the California Law Enforcement Telecommunications System (CLETS) and the California Department of Motor Vehicles (DMV) is confidential, for official use only, and is based on the 'need to know' and 'right to know' in accordance with assigned duties. The misuse of information from these systems may adversely affect an individual's civil rights and violates the law and/or CLETS and DMV policy. UPD employees who access or who may have access to this information must sign a CLETS Employee/Volunteer Statement Form and a DMV Information Security Statement, signifying that the employee has read and understands the policies involving use of this information.

The Agency CLETS Coordinator shall ensure that each employee completes the statement within thirty (30) days of hire, and in January of each succeeding year. The completed forms will be retained by the Agency CLETS Coordinator for two full calendar years following the employee's date of termination or separation from the University Police Department.

342.8 UPD INFORMATION SECURITY

342.8.1 INTRODUCTION:

Information Resources are strategic assets of the University Police Department (UPD) and must be treated and managed as valuable resources. The UPD provides various computer resources to its employees for the purpose of assisting them in the performance of their job-related duties.

342.8.2 ROLES AND RESPONSIBILITIES:

- UPD management will follow the periodic reporting requirements established by the Cal Poly Information Security Officer to measure the compliance and effectiveness of Information Security policies.
- UPD management is responsible for implementing the requirements of Information Security policies and documenting non-compliance as directed by the Information Security Officer.
- UPD Managers, as directed by the Information Security Officer, are required to monitor the training of employees on Information Security polices and document issues with policy compliance.

- All UPD employees are required to read and acknowledge the reading of this policy.

342.8.3 POLICY DIRECTIVES:

Data Security

Cal Poly retains ownership or stewardship of information assets owned (or managed) by or entrusted to Cal Poly. Cal Poly reserves the right to limit access to its information assets and to use appropriate means to safeguard its data, preserve network and information system integrity, and ensure continued delivery of services to users. This can include, but is not limited to: monitoring communications across campus network services; monitoring actions on the campus information systems; checking information systems attached to the campus network for security vulnerabilities; disconnecting information systems that have become a security hazard; or, restricting data to/from campus information systems and across network resources. These activities are intended to protect the confidentiality, integrity and availability of information, and are not intended to restrict, monitor, or utilize the content of legitimate academic and organizational communications.

Cal Poly performs periodic assessments of its information security risks and vulnerabilities. Risk assessments may be aimed at particular types of information, areas of the organization, or technologies. Risk assessments are part of an ongoing risk management process. They provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of campus controls. The Cal Poly Security Risk Self-Assessment and Inventory Standard contains processes to perform annual self-assessments and inventory reporting.

The Security Risk Self-Assessments and Inventories are requested, collected, reviewed and evaluated by the Information Security Officer and the Vice Provost/Chief Information Officer. The results are shared with executive management and campus computing committees. The outcomes are produced in a Risk Assessment Report updated annually identifying control objectives, risk exposures, mitigation strategies and action plans for addressing each risk with timelines.

AFD conducts a vulnerability assessment of all of their networked computing devices on a periodic basis as directed by the Information Security Officer. Specifically, monthly scans are required for the following networking computing devices:

Any university computing devices that are known to contain Level 1 data

Any university computing devices that must meet specific regulatory requirements, e.g., PCI, HIPPA, etc.

All file-system images or virtual machine templates used as base images for building and deploying new workstations or servers

All devices that are used as servers or used for data storage

Any network infrastructure equipment

Cal Poly Information Classification and Handling Standard

AFD Patching Policy

Cal Poly Vulnerability Assessment and Management

AFD Vulnerability Policy

The Cal Poly Security Risk Self-Assessment and Inventory Standard

Access to Network Equipment

Access to campus information assets containing protected data as defined in the Cal Poly Information Classification and Handling Standard may be provided only to those having a need for specific access in order to accomplish an authorized task. Access must be based on the principles of business need and least privilege.

Authentication controls must be implemented for access to campus information assets that access or store protected data, must be unique to each individual and may not be shared unless authorized by appropriate the Information Security Officer or the Vice Provost/Chief Information Officer. Where approval is granted for shared authentication, the requesting organization must be informed of the risks of such access and the shared account must be assigned a designated owner. Shared authentication privileges must be regularly reviewed and re-approved in writing at least annually.

All AFD hosted network resources require Active Directory authentication for access. Access is controlled by group membership assigned by departmental and business functional "roles". Password security complies with Cal Poly and CSU standards for complexity and failed login lockout procedures. Login to and logoff from AFD workstations and servers is logged to a central database with records retained for at least 90 days, longer when directed by Cal Poly security policies. Idle devices have password protected screen savers enabled. The AFD Sessions Locked After Inactivity policy delineates the idle times by class of computing device. For the UPD, the idle time is 15 minutes with the exception of Dispatch workstations which are exempt but have mitigating controls: (a) are continuously manned, (b) locked spaces with managed access to outside spaces, (c) required to be available for safety reasons, and (d) utilize secondary firewall protection isolating the Dispatch workstations from the campus network.

Cal Poly Devices Security Information

Cal Poly Computing Devices Standard

Department of Justice Terminals

Conforms to the CLETS Policies, Practices and Procedures Manual and to Cal Poly and CSU Information Security Standards where applicable.

Computer-Aided Dispatch/Record Management Systems

Conforms to Cal Poly and CSU Information Security standards

Data Backup and Storage

Data backup and storage of backup files is managed by the AFD Network and Technology Services group.

- A full local backup of the CAD database is performed every day by the database engine. Incremental local backups of the database are performed every two hours by the database engine.
- A full network backup of the CAD server is performed weekly. All network backups are encrypted and stored off site for three weeks. One weekly backup each month is kept offsite an additional month. An incremental backup of the CAD servers is done nightly after the SQL backups are completed. Incremental backups are encrypted and stored off site with their accompanying full backup.
- A full local backup of the T2 FLEX database is performed nightly.
- A full network backup of the T2 FLEX database and e-business servers are performed weekly and incremental backups are performed nightly.
- A full network backup of the server hosting the departmental file share is performed weekly and incremental backups are performed nightly. The Shadow Copy Service is enabled for this file server.
- AFD workstations are not backed up. As a matter of policy, departmental data files are not to be stored locally for security and recovery reasons.

Passwords

Active Directory password policies conform to Cal Poly and CSU Information Security standards.

- A strong password must be used for all devices supporting authentication and password authenticated services connected to the campus network.
- To be considered strong, passwords must conform to the rules established for the Cal Poly Password regarding complexity, length, and composition as described below.
- If this is not technically feasible, the strongest possible password rules must be implemented.
- Strong passwords must be changed at least once annually (every 365 days). More frequent changes may be required for resources that do not support strong passwords (i.e., does not conform to the Cal Poly Password rules).
- Well known or publicly posted identification information must not be used as a password.
- Input of all passwords must be masked.
- Passwords must be encrypted during storage and transmission over networks Passwords must not be stored in clear text or a readily decrypted form.
- Passwords must be stored in a non-reversible format.

- Embedding or hard-coding passwords into any system must be avoided whenever possible.
- University approved electronic password safes may be used to store additional passwords as long as an appropriate strong password is utilized for the safe.
- Devices must not be configured allowing logins without a password. Exceptions may be granted for specialized devices such as kiosks which have extremely restricted accounts.
- Passwords must be changed whenever a system or account is suspected of being compromised, and the incident must be reported to abuse@calpoly.edu.
- All default passwords for access to network-accessible devices, applications and services must be modified at installation to one that complies with this standard.
- Any pre-assigned passwords must be changed immediately upon initial access to the account.
- Unless other mitigating controls exist, separate passwords must be used for privileged and unprivileged access by the same user on the same device. Mitigating controls may include security controls built into the operating system or authentication services, for example.
- Use of privileged access passwords must be limited to system administration activities only.
- Account and password management functions must be restricted to authorized staff.
- After four (4) incorrect password tries within 33 minutes, access must be denied automatically. The access must be denied for 33 minutes or until the account is manually reset by authorized staff. Note: Active Directory is configured to allow six incorrect password attempts with a lockout of 3 days.
- Password change procedures must authenticate the user prior to changing the password. Acceptable forms of authentication include answering a series of specific questions whose answers would not be known except by the user and trusted staff, showing one or more forms of photo ID, etc.
- After a password reset by authorized staff, a password change is required within three (3) days. Note: for Active Directory the password change is set for next login.
- Administrative passwords must be changed whenever there is a change in administrator.
- Administrative passwords must be on file with the employee's supervisor or readily accessible by the supervisor in the event of an emergency or the administrator is not available.

- Administrative passwords must be unique from other passwords used by the individual.
- Use of administrative passwords must be limited to system administration activities only. Administrative passwords must be disabled or returned to the appropriate department or entity on demand, upon termination of the relationship with the university, or when an employee no longer requires administrator access as part of their job duties and responsibilities.
- Administrative passwords may be stored in a secured electronic location with limited access.
- Administrative passwords should be changed as frequently as is warranted based on risk.
- Passwords must contain at least one character from three of the following lists:

1. Uppercase Alphabetic (A-Z)

2. Numbers (0-9)

3. Lower case Alphabetic (a-z)

4. Special Characters: ! $ % & , ( ) * + - . / ; : ? [\ ] ^ _ { } ~m = 'less than' symbol, 'greater than' symbol

Passwords must not contain any of the following:

1. Your previous passwords used within the last two (2) years

2. Passwords less than 16 characters must not contain any of the following:

a. Any words of three or more characters, including non-English words

b. Any groups of three or more characters of the same character type

c. Any names, person, places, or things found in a common dictionary

d. Any of your names (first, middle, last), any current Cal Poly username

e. Repetitive characters (sequences)

Note: Active Directory configured to not allow the most recently used 24 passwords. Active Directory does not fully enforce all of these complexity requirements.

Cal Poly Security Standard: Passwords

Account Provisioning

Active Directory, CAD and T2 FLEX account provisioning conforms to Cal Poly and CSU Information Security standards.

Required:

A user account must only be used by the person to whom it is assigned.

The processes to create and terminate user accounts must be approved and documented by an authorized owner of the system, application, or database. A list of authorized owners must be documented and maintained.

Nobody is allowed to authorize their own access. Administrators who have access to add or elevate their own privileges must have mitigating procedures in place for logging changes to production systems containing Level 1 and Level 2 data.

The principle of least privilege is to be used in granting access. In particular, Administrative access is not to be granted unless required to maintain system integrity, confidentiality, and availability.

User account access to view, change or delete information must be disabled or deleted when no longer required. This can be accomplished through changes in authorization (privileges granted to an account) or removal of the account itself if no privileges are required.

Periodic reviews and documented signoffs of Cal Poly employee user accounts providing access to Level 1 or Level 2 data must be performed on a regular basis, at least annually. Annual signoffs on automated processes for populations such as students or alumni can be done if the process is approved by the ISO. Triggering events require immediate review of access be performed by the Authorized Owner or appropriate approving authority. These events include position change or termination.

User accounts can be suspended at any time if requested by an appropriate representative in the respective department or College, the Chief Information Officer, or Information Security Officer. Unless otherwise authorized, a user's account must be disabled by the user's last day of employment or other relationship with the University.

Recommended:

Disable accounts with access to Level 1 or Level 2 data that have not been accessed since the last required review period.

Administrator accounts should only be used for tasks that require administrative privileges.

System Administrators must take care to ensure that user access is approved and necessary for operational purposes.

Integrated CSU Administrative Manual §8060.0

Cal Poly Security Standard: Managing Computer Accounts

AFD Access to be Assigned by Role Policy

AFD 30 Day Account Review Policy

AFD Disable Account(s) in Event of System Compromise Policy

Annual Review of Access Rights

Conforms to Cal Poly and CSU Information Security standards. AFD Network and Technology Services group reviews folder access with managers during the spring quarter each year.

AFD Annual Review of Folder Security

Training

Information Security Awareness and Training consistent with CSU Information Security Policies, all employees with access to the Cal Poly network and information assets must participate in information security awareness training.

The Information Security Awareness Training Program is designed to help individuals protect and respond appropriately to threats to campus information assets containing level 1 or level 2 data as defined in the Cal Poly Information Classification and Handling Standard.

The Program promotes awareness of:

- CSU and campus information security policies, standards, procedures, and guidelines.
- Potential threats against campus protected data and information assets.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information assets.
- CSU and campus notification procedures in the event protected data is compromised. Within about one month of employment, new employees are provided individual access to the Information Security Awareness Training Program.

Employees are expected to complete the training within 90 days of receiving their access to the Program. Department heads and campus executive management are responsible for and will be provided status of training compliance.

Cal Poly Information Security Training Handout

Integrated CSU Administrative Manual §8035.0

342.8.4 ENFORCEMENT, AUDITING, REPORTING:

1. Violation of this policy may result in disciplinary action that may include termination for employees and temporaries; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers. Additionally, individuals are subject to loss of UPD information resources access privileges, civil, and criminal prosecution.

2. UPD Management is responsible for the periodic auditing and reporting of compliance with this policy as required by the Cal Poly Information Security Officer.

3. Exceptions to this policy will be considered only when the requested exception is documented as required by the Cal Poly Information Security Officer.

342.8.5 REFERENCES:

In addition to Federal and State statutes, the UPD is subject to Information Security Policies promulgated by the California State University and Cal Poly. California State University policies are specified in Section 8000 of the Integrated CSU Administrative Manual. Cal Poly University security policies are specified in the Cal Poly Information Security Program and the Responsible

Use Policy. Additionally the Cal Poly Administration and Finance Division issues detailed policies and procedures to expand upon these policies.

Links Integrated CSU Administrative Manual §8000 http://www.calstate.edu/icsuam/sections/8000/

Cal Poly Information Security Program http://www.security.calpoly.edu/sites/security/files/docs/policy/isp.pdf

Cal Poly Information Classification and Handling Standard http://security.calpoly.edu/content/policies/standards/classification/index

AFD Patching Policy O:\ANTS\LAN\Network\POL-Patching.docx

AFD Vulnerability Policy O:\ANTS\Support\Software\Qualys\REF-Vulnerability Scans.docx

The Cal Poly Security Risk Self-Assessment and Inventory Standard http://www.security.calpoly.edu/content/policies/standards/risk/index

Cal Poly Vulnerability Assessment and Management http://www.security.calpoly.edu/content/vulnerability

AFD Sessions Locked After Inactivity O:\ANTS\Security & Access\Policies\POL-Sessions Locked After Inactivity.docx

Cal Poly Devices Security Information O\ANTS\Security & Access\Security\Information Security Docs\AFD - Devices Security Information.xlsx

Cal Poly Computing Devices Standard http://security.calpoly.edu/sites/security/files/docs/standards/device.pdf

CLETS Policies, Practices and Procedures Manual O:\ANTS\Security & Access\Security\CLETS Policies, Practices and Procedures Manual 20121203.pdf

Cal Poly Security Standards: Passwords http://security.calpoly.edu/sites/security/files/docs/standards/passwords.pdf

Cal Poly Security Standard: Managing Computer Accounts http://security.calpoly.edu/sites/security/files/docs/standards/accounts.pdf

AFD Access to be Assigned by Role Policy O:\ANTS\Network & Servers\Networking\POL-Access to be Assigned by Role.docx

AFD 30 Day Account Review Policy O:\ANTS\Application Administration\Active Directory\User & Service Accounts\ REF-30 Day Account Review.docx

AFD Disable Account(s) in Event of System Compromise O:\ANTS\Network & Servers\Networking\REF-Disable Account(s) in Event of System Compromise.docx

AFD Annual Review of Folder Security O:\ANTS\Security & Access\Folder Security Reports\POL-Annual Review of Folder Security.docx

Cal Poly Information Security Training Handout http://security.calpoly.edu/security/sites/wcms.calpoly.edu.security/files/docs/isat/InfoSecurityTraining_Handout_Final.pdf

342.8.6 CONTROL AND MAINTENANCE:

The UPD Information Security Polices will be reviewed and revised at least annually and as required by the Cal Poly Information Security Officer.