AP 3725 PCCD Information Technology Security Standard

Contents

1. Managerial and Administrative Security

1.1. Managerial Security[1]

1.1.1. Responsibility for Information Security[2]

A. It is the responsibility of all employees to be aware of the security policy and to adhere to its procedures. However, one employee must be assigned the ultimate responsibility of ensuring

[1] HIPAA Security Standards: Administrative Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/adminsafeguards.pdf
[2] NIST 800-3 PM2 - Senior Information Security Officer - https://nvd.nist.gov/800-53/Rev4/control/PM-2

that the community college district policy is implemented, clearly communicated, and kept up to date. This employee should be given the title of Senior Technology Officer (STO)

B. The STO must ensure:
    1. security policies and procedures are established, documented and distributed
    2. Security alerts and information are monitored and analyzed
    3. Incident response and escalation procedures are established, documented and distributed in order to ensure timely and effective identification and appropriate handling of all security events
    4. User accounts and access privileges are appropriately administered (including additions, deletions and modifications)
    5. All access to data is monitored and controlled
    6. Risk and technical assessments are performed regularly
    7. Controls are adequately implemented to mitigate risk
    8. Personnel are appropriately trained with respect to information security risks and practices
    9. Vendors, tools and services are assessed in order to determine business risk

1.1.2. Security Policy Requirements[3]

A. Peralta must ensure all employees and contractors that have access to Peralta information and assets are informed of the security policy.
B. All security-related policies must be approved by the STO.
C. The General Information Security Policy must be reviewed at least annually, and the Policy must be updated after any relevant event changes to the district or the assets.

1.1.3. Use of Information Security Assets[4]

A. Technologies and systems specific to information security, such as vulnerability scanning, intrusion detection, and penetration testing tools may only be used by personnel who are authorized by the STO to use such technologies and systems.

1.1.4. Security Committee

A. There is a committee of appointed employees called the Peralta Security Committee. This committee is headed by the STO and filled with key members of each school as well as the district. The purpose of this committee is to ensure each campus, as well as the district office, complies with secure standards and that the security policy is adequate for their respective needs. This committee meets on a regular schedule to oversee the following topics:
    1. Review and approval of information security policies
    2. Monitoring significant changes in risk for the district
    3. Review of any security incidents
    4. Involvement in major initiatives to improve security
    5. Raising and resolving employees' and PCCD community questions and issues

[3] NIST 800-53 PM1 – Information Security Plan - https://nvd.nist.gov/800-53/Rev4/control/PM-1
[4] NIST 800-53 AC1 – Access Control - https://nvd.nist.gov/800-53/Rev4/control/PM-1

1.1.5. Business Continuity and Disaster Recovery

A. Peralta District must implement and maintain a Business Continuity and Disaster Recovery (BCDR) plan.
B. The BCDR plan must include the following:
    1. Impact analysis (identification and prioritization of systems and important components)
    2. Periodic media backups cycled to offsite storage
    3. Controlled access to, and storage of, media (including backups)
    4. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) information
        - RPO: Days worth of lost productivity that the institution can recover from.
        - RTO: maximum tolerable length of downtime that the institution can recover from.
    5. Disaster Recovery plan location and migration procedures
    6. Roles & responsibilities and contact information for critical parties
    7. Business and computer contingency plans covering hardware, software, communications, staff and key business functions
    8. An incident management plan
    9. Inventories of key system components
    10. A basic communication plan
C. The Peralta Community College District must test the Business Continuity and Disaster Recovery plan at least annually.
D. Disaster Recovery systems and other resources must be protected using appropriate security measures in accordance with this policy.

1.2. Administrative Security

1.2.1. Policy Exceptions

A. It is likely that issues will come up where it will be necessary to operate outside of the security policy, the Peralta Community College District will allow the STO to approve policy exceptions. These may only be issued if they are necessary for the Peralta Community College District to operate as mandated by the Board of Trustees.
B. Policy exceptions must be approved by the STO and must be for a specific duration.
C. Policy exceptions must be reviewed at least annually in order to determine if the exception should continue to exist.

1.2.2. Acceptable Use[5]

A. Users must comply with Peralta's Acceptable Use Policy to use any of the PCCD's resources.

1.2.3. Identifying Security Vulnerabilities

A. It is the responsibility of the STO and any employees in an administrator role to remain current with trends in security threats that apply to the Peralta Community college district.

[5] NIST 800-53 – Access Agreements - https://nvd.nist.gov/800-53/Rev4/control/PS-6

B. Any applicable vulnerabilities identified must be assigned by the STO a risk rating (e.g.: low, medium, high, and critical.
C. Security vulnerabilities must be addressed by the STO in accordance with their risk rating; higher risk vulnerabilities have a higher priority.

1.2.4. Training and Awareness[6]

A. Information security is an important and mandatory part of any faculty or staff's training at the Peralta Community College District. There will be training seminars at least once per academic year as well as communication newsletters when pertinent information is released.
B. All newly hired employees will be trained on best practices for information security at the time of hire.
C. All employees must sign and acknowledge that they have received security training and understand their responsibilities.
D. In addition to training at the time of hiring, all employees must undergo refresher courses once per academic year and sign and acknowledge that they are current as of that training and understand their responsibilities.

1.2.5. Training for Software Development Staff

A. Software Development and Quality Assurance staff who develop or test important software (e.g.: web applications, backend code, any software that performs and processes customer, consumer or third party data and any software that handles Sensitive Information such as Confidential or Highly Restricted Data) must receive annual application security training. This training must address the most common software vulnerabilities, including those outlined in the current OWASP Top Ten.[7] The training will also provide an understanding of how sensitive data is processed in memory.

1.2.6. Reporting Security Problems

A. A Security Incident is any suspected or confirmed violation of Peralta' Information Security policies. This includes, but is not limited to: system compromises, virus infections, phishing emails, social engineering attacks, lost company assets (e.g.: mobile phone with company data, hard copy documents containing company data, etc.)
B. <u>All Security Incidents including lost information assets, must be reported to IT immediately.</u> The best way to report a Security Incident is to email Helpdesk@Peralta.edu or open a Helpdesk ticket.

[6] NIST 800-53 – Awareness and Training Controls - https://nvd.nist.gov/800-53/Rev4/family/Awareness%20and%20Training
[7] Open Web Application Security Project - Lists the top 10 most critical security threats - https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

1.2.7. Incident Response Plan[8]

A. Peralta must create and maintain a Security Incident Response Plan. The plan must detail the processes to be followed if a security incident occurs, timelines for response and escalation, a basic communication plan and a retrospective/post-mortem process and timeline.

1.2.8. Risk Assessment[9]

A. A risk assessment must be performed at least annually and after any significant changes to the environment (e.g.: acquisition, merger, relocation, etc) by the STO in junction with the Risk Management department.
B. Risk assessments must identify critical assets, threats and related vulnerabilities.
C. Vulnerabilities must be assigned an appropriate risk level (e.g.: Likelihood x Impact == Risk) by the STO in junction with the Risk Management department.
D. The Risk Assessment process must be based on an industry-accepted methodology and include the following:
    1. Determination of scope
    2. Threat & vulnerability identification
    3. Control analysis
    4. Determination of likelihood and analysis of impact for each vulnerability
    5. Determination of risk for each identified vulnerability
    6. Control recommendation and documentation of results
    7. Requirements for ongoing monitoring of identified risks
E. The Risk Assessment process must result in a formal Risk Assessment document.
F. The Risk Assessment should be used to determine prioritization of security-related work for the following 12 months.

1.2.9. Asset Management[10]

A. The IT team is responsible for creating and maintaining an inventory of all assets that store, process or transmit confidential data.
B. The asset inventory must be updated at least quarterly and when new hardware is deployed, decommissioned or repurposed.
C. The asset inventory must always capture the following information:
    1. Owner/maintainer
    2. Make, model of device
    3. Location of device (address or facility)
    4. Device serial number or other method of unique identification
    5. Business function of device
    6. Classification of data stored, processed or transmitted by the device (e.g.: Public or Confidential)

---

[8] NIST 800-53 IR-8 – Incident Response Plan https://nvd.nist.gov/800-53/Rev4/control/IR-8
[9] NIST 800-53 RA1/RA3 Risk Assessment - https://nvd.nist.gov/800-53/Rev4/control/RA-1, https://nvd.nist.gov/800-53/Rev4/control/RA-3
[10] NIST 800-53 CM-8 Configuration Management - https://nvd.nist.gov/800-53/Rev4/control/CM-8

D. Maintenance of the asset inventory will be done by Campus and District Helpdesks and District Warehouse.

1.3. Personnel Security

1.3.1. IT Processes Discipline and Termination[11]

A. Violators of Peralta's General Information Security Policy and any related policies and procedures are subject to disciplinary measures, including privilege revocation and/or employment termination. Actions that may result in disciplinary measures include, but are not limited to, accessing any PCCD computer systems or data in an unauthorized manner or in access outside of granted privileges.
B. All user accounts associated with terminated employees must be disabled or deleted within 24 hours of the employee's termination.
C. Procedures for employee terminations include assigned management responsibility, escorted departures for terminations for cause, exit interviews, and a detailed termination checklist.
D. Disciplinary measures will not exempt employees of civil or criminal liability.

2. Software and System Security[12]

2.1.1. Passwords[13]

A. All newly created passwords must be a minimum of 16 characters (e.g. thegreatorangegoat). [1]
    1. Don't use any part of your name
    2. Don't use the same word more than once
    3. Don't use words that relate to your work or occupation.
    4. Do use as unique a phrase as possible.
B. New or changed passwords shall be compared against a list that contains commonly-used, expected, or compromised passwords.
C. The account will lock after a determined number of attempts.
D. Passwords must not be stored on any electronic device unencrypted.
E. If passwords are written down, they must be stored in a secured location away from any device that may use that password (not in line-of-sight).
F. Do not reveal your password with anyone, including co-workers and supervisors. If someone demands a password, refer them to this document or have them call your IT department.

2.1.2. Password Deletion

A. The following conditions require that an account's password be disabled or deleted. This includes, but is not limited to:
    1. When a user retires, quits, is dismissed or released.

---

[11] NIST 800-53 PS-4 – Personnel Termination - https://nvd.nist.gov/800-53/Rev4/control/PS-4
[12] HIPAA Security Standards: Technical Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/techsafeguards.pdf
[13] NIST 800-63B , section 5 - Digital Identity Guidelines - https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

2. Contractor accounts when the account or access is no longer needed to perform their duties.

B. The following procedures shall take place when a password is no longer needed:
   1. The user shall notify their immediate supervisor.
   2. The contractor shall notify their Point of Contact (POC).
   3. The supervisor or POC shall notify District IT that the user's password and/or account requires deletion or disabling.

2.1.3. User Management[14]

A. All Peralta District users and contractors are granted access to data and systems based on a need-to-know and "least privilege level" basis. Users must be granted only the minimum privileges necessary to perform job responsibilities.

B. All Peralta District users and contractors requiring access to any confidential data must obtain documented approval to gain access, and list the specific privileges approved.

C. Peralta District shall use role-based access control where available. Where possible, roles must be defined for each job responsibility. Access needs and privilege assignments must be documented for each role. Roles must represent the individual personnel's job classification and function.

D. Group and/or shared accounts are explicitly prohibited.

E. Windows administrators shall not use an account with Domain Admin privileges for typical user activities.

2.1.4. Access Controls & Privilege Management[15]

A. Multi-factor authentication (MFA) helps prevent unauthorized use by requiring two distinct forms of identity (e.g. something you know and something you have) when logging into networks or systems that access confidential data. Employees, students, and contractors of Peralta Community College District shall use Multi-Factor Authentication when accessing networks or systems that access confidential data.

B. Periodic review of access privileges shall take place to ensure that personnel are assigned the appropriate access permissions as a coordinated effort between Human Resources and the IT department.

2.1.5. Patch Management[16]

A. Regular security updates and patches of vendor applications are necessary to protect Peralta District systems and data from malicious attacks and software malfunction. All system components and software shall be protected from known vulnerabilities by installing applicable vendor supplied security patches.

---

[14] NIST 800-53 AC-5, AC-6 Access Control - https://nvd.nist.gov/800-53/Rev4/family/Access%20Control
[15] NIST 800-53 AC-2 Account Management - https://nvd.nist.gov/800-53/Rev4/control/AC-2
[16] NIST 800-53 SI-2: Flaw Remediation - https://nvd.nist.gov/800-53/Rev4/control/SI-2

2.1.6. System Configuration Standards & Hardening[17]

A. Critical computer systems and components such as network devices and databases must have system configuration standards that are maintained and implemented.
B. System configuration must use industry-accepted system "hardening" standards to ensure that a minimum baseline security standard is met. This standard must also address all known security vulnerabilities.
C. Sources of industry-accepted system hardening standards include, but are not limited to:
    1. Center for Internet Security (CIS)
    2. International Organization for Standardization (ISO)
    3. SysAdmin Audit Network Security (SANS) Institute
    4. National Institute of Standards Technology (NIST).
D. System configuration standards must be updated as new vulnerabilities are identified.
E. System configuration standards must be applied when new systems are configured and verified as being in place as part of the system deployment process
F. System configuration standards must address security policies and operational procedures for managing vendor defaults and other security parameters.
G. Daily monitoring of systems shall occur to ensure that maintenance of the baseline configuration standards.

2.1.7. Audit Log Management[18]

A. Audit trails should be implemented on systems that transmit, process, or store confidential data to link individual user's access to system components.
B. Audit trails must be maintained for at least one year with the most recent three months available online.

2.1.8. Removable Media[19]

A. Confidential Data must not be stored on removable media (e.g.: USB thumb drives, CD/DVD ROM and other optical media, etc.) unless it is encrypted in accordance with section 2.3.4 of this document.

2.1.9. Change Control[20]

A. Production changes must be documented, reviewed, assessed for risk/priority, and approved prior to implementation.
B. Security patches and software modifications must be documented.
C. Test accounts or test data must be removed after testing requirements are completed.

---

[17] NIST 500-53 CM-6 Configuration Settings https://nvd.nist.gov/800-53/Rev4/control/CM-6
[18] NIST 800-53 AU-6 - Audit Review Analysis and Reporting - https://nvd.nist.gov/800-53/Rev4/control/AU-6
[19] NIST 800-53 MP-7 Media Use https://nvd.nist.gov/800-53/Rev4/control/MP-7
[20] NIST 800-53 – Configuration Management Control - https://nvd.nist.gov/800-53/Rev4/family/Configuration%20Management
NIST 800-53 – MA-2 Controlled Maintenance - https://nvd.nist.gov/800-53/Rev4/control/MA-2

2.2. Security Monitoring[21]

2.2.1. Network Intrusion Detection Systems

A. Network traffic that transitions between the production environment and the Internet must be analyzed by a Network Intrusion Detection System (NIDS) that inspects the traffic for evidence of malicious activity (e.g.: port scans, hacking attempts and denial of service (DoS) attacks).
B. The NIDS must operate 24x7 and report detected issues as quickly as the system configuration allows.
C. The NIDS must be able to perform protocol analysis, content searching & matching and must be able to detect common attacks and pre-attack probes. This includes, but is not limited to, buffer overflows, stealth port scans, operating system fingerprinting attempts and common web application security attacks.
D. The NIDS alerts must be monitored in accordance with sections 2.7 Security Alerts and 2.8 Security Event Review.

2.2.2. Host-based Intrusion Detection Systems

A. Systems that store Confidential data should be protected by a Host-based Intrusion Detection System (HIDS).
B. HIDS software must monitor system events (24x7) in near-real time and generate alerts for activity that indicates a possible Security Incident.
C. The HIDS alerts must be monitored in accordance with sections 2.7 Security Alerts and 2.8 Security Event Review.

2.2.3. File Integrity Monitoring

A. File Integrity Monitoring (FIM) is the process of periodically recording and comparing cryptographic fingerprints of files for evidence of changes to those files.
B. Critical system files (e.g.: /etc/password on Linux systems and OS-level logs), configuration management files (e.g.: Salt configuration files) and application-critical files (e.g.: application logs, application configuration/properties files) must be checked at least daily by File Integrity Monitoring software.
C. The FIM software must be configured to generate an alert when the contents of monitored files change.
D. The FIM alerts must be monitored in an appropriate timely manner.

2.2.4. Malicious Software & Anti-virus

A. Systems must have anti-virus and anti-malware software installed and running with the latest available signatures while the computer is operating.
B. Systems that require anti-virus and anti-malware software are:
    1. Computers running any Microsoft Windows operating system
    2. Computers running any Apple OS X operating system (excluding mobile devices)
C. All anti-virus and anti-malware mechanisms must be maintained as follows:

[21] NIST 800-53 SI-4 Information System Monitoring - https://nvd.nist.gov/800-53/Rev4/control/SI-4

1. Must be configured to check for and apply updates at least daily
2. Must perform whole system scans at least weekly
3. Must generate audit logs which are retained in accordance with this policy (at least one year of log data must be available at all times, with the most recent three months available online) and all applicable laws and industry rules & regulations

D. Users must not disable anti-virus or anti-malware software without documented approval by the Peralta IT Department.
E. Users must immediately report to Peralta IT Department any of the following:
    1. Anti-virus/anti-malware software isn't updating correctly
    2. Anti-virus/anti-malware software isn't running
    3. Anti-virus/anti-malware software indicates a compromise
F. Systems that are not traditionally subject to malware infection must be re-evaluated at least annually to ensure that anti-virus/anti-malware software is still not applicable to those systems.

2.2.5. Rootkit Detection

A. Systems that store confidential data should have rootkit detection software installed.
B. Rootkit detection software must run at least daily and must generate alerts for detection of possible rootkits.
C. The rootkit detection software alerts must be monitored in an appropriate and timely manner.

2.2.6. Centralized Logging[22]

A. Systems that store, process or transmit Confidential Data should send audit trails to a centralized log server or to other media that is difficult to alter and otherwise protected from tampering.
B. Security-specific monitoring devices and all external-facing technologies in the production environment (e.g.: firewalls, DNS, mail) must send their logs to a centralized log server or other media that is difficult to alter and otherwise protected from tampering.

2.2.7. Security Alerts

A. The IT team is responsible for 24x7 monitoring, analyzing and driving resolution of security alerts.
B. All security alerts must be rated for Risk (e.g.: Critical, High, Medium, Low or Likelihood x Impact = Risk).
C. Security alerts must be reviewed, tracked and resolved in a timely manner by the IT department:
    1. Critical risk alerts must be resolved as soon as possible
    2. High risk alerts must be resolved within 24 hours of detection
    3. Medium risk alerts must be resolved within one month of detection

2.2.8. Security Event Review

A. The Peralta IT Department is responsible for monitoring security-related events.
B. The following must be monitored at least daily:

[22] NIST 800-53 Audit Generation https://nvd.nist.gov/800-53/Rev4/control/AU-12

1. All security events
2. Logs of all system components that store, process, or transmit confidential data, or that could impact the security of confidential data
3. Logs of all critical system components
4. Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

C. Logs of all other system components must be reviewed at least monthly.

2.3. Security Assessments[23]

2.3.1. Vulnerability Scanning

A. Peralta District must perform internal and external vulnerability scanning at least quarterly and after any material changes to the environment (e.g., new system component installations, changes in network topology, major firewall rule modifications, product upgrades, etc.)
B. The Peralta IT Department is responsible for scheduling and performing periodic vulnerability scans, selecting vulnerability scanning tools/vendors, reviewing vulnerability scan results and resolving issues brought up by vulnerability scan findings.
C. Internal vulnerability rescans must be performed until all high and critical risk vulnerabilities are resolved.

2.3.2. Penetration Testing[24]

A. Peralta District must undergo periodic penetration testing that is based on industry-accepted penetration testing approaches (e.g.: NIST SP800-115) and is performed by a trusted, skilled third-party tester.
B. The Peralta IT team is responsible for scheduling periodic penetration tests, selecting testers, reviewing results and driving resolution of penetration test findings.
C. Penetration tests must be performed annually and after any material changes to the environment (e.g., new system component installations, changes in network topology, major firewall rule modifications, product upgrades, etc.)
D. The Vice Chancellor of IT is responsible for determining the scope of penetration tests.
E. Penetration test results must be retained for at least three years.
F. Exploitable vulnerabilities found during penetration testing must be corrected in accordance with their risk level.

[23] NIST 800-53 Security Assessment and Authorization - https://nvd.nist.gov/800-53/Rev4/family/SECURITY%20ASSESSMENT%20AND%20AUTHORIZATION
[24] NIST 800-53 CA-8 Penetration Testing - https://nvd.nist.gov/800-53/Rev4/control/CA-8

2.3.3. Communications Security

2.3.3.1. External Network Connections

A. Peralta District internet connections must be protected by properly configured and monitored firewalls.
B. The Peralta District network must be segmented into logical domains.
C. New connections to the Peralta District network may only be added under controlled circumstances, in accordance with the Change Control policy, and must be approved by the STO.

2.3.3.2. Remote Access[25]

A. Specific approval for remote access to the Peralta District network must be obtained from District IT.
B. Successful authentication via a two-factor user authentication technology is required to establish a remote access connection (e.g.: VPN) to the Peralta District network.
C. Certificates, passwords and other authentication tokens must be unique to each user account.
D. All remote access to Peralta District network must be encrypted, including the authentication and authorization steps, using encryption standards as defined in section 2.3.4 of this document.
E. Remote access to Peralta District network must be monitored by the IT team.
F. Remote access sessions must be disconnected after no more than 4 hours of inactivity.
G. Remote access sessions must have a maximum lifetime of 24 hours regardless of activity.
H. Remote access technologies used by vendors and business partners may only be activated when necessary, with immediate deactivation after use.

2.3.3.3. Firewalls and Access Control Lists[26]

A. Stateful inspection packet filtering firewalls (a network firewall that tracks the operating state and characteristics of network connections traversing it) must inspect traffic passing between any Peralta District network and the Internet and between any demilitarized zone (DMZ) and internal network zones.
B. The Peralta IT team is responsible for managing firewalls in accordance with Peralta District security policies.
C. Peralta District Change Control process must be followed for approving and testing all network connections and changes to the firewall and router configurations.
D. Any network that stores, processes or transmits Confidential Data is a Confidential Data Environment.
E. The IT team must maintain a current network diagram that identifies all connections between networks that hold confidential data and other networks, including any wireless networks.
F. The IT team must maintain a current diagram that shows all confidential flows across systems and networks.

---

[25] NIST 800-53 AC-17 Remote Access - https://nvd.nist.gov/800-53/Rev4/control/AC-17
[26] NIST 800-53 Systems and Communications Protection - https://nvd.nist.gov/800-53/Rev4/family/System%20and%20Communications%20Protection

G. The IT team must maintain a description of groups, roles, and responsibilities for management of network components.
H. The IT team must create and maintain documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. Examples of insecure services, protocols, or ports include but are not limited to FTP, Telnet, POP3, IMAP, and SNMP v1 and v2.
I. The IT team must review firewall and router rule sets at least every six months.
J. The IT team must build firewall and router configurations that restrict connections between untrusted networks and any system components in the confidential data environments.
K. The IT team must restrict inbound and outbound traffic to that which is necessary for the confidential data environments, and specifically deny all other traffic.
L. The IT team must secure and synchronize router configuration files.
M. The IT team must install perimeter firewalls between all wireless networks and confidential data environments, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and confidential data environment.
N. The IT team must prohibit direct public access between the Internet and any system component in the confidential data environment by doing the following:
    1. Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
    2. Limit inbound Internet traffic to IP addresses within the DMZ.
    3. Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)
    4. Do not allow unauthorized outbound traffic from the confidential data environment to the Internet.
    5. Implement stateful inspection (e.g.: only “established” connections are allowed into the network.)
    6. Place system components that store confidential data (e.g.: databases) in an internal network zone, segregated from the DMZ and other untrusted networks.
    7. Do not disclose private IP addresses and routing information to unauthorized parties (e.g.: by use of NAT to hide internal addresses from outside parties).

2.3.3.4. Host-based Firewall

A. All laptops and employee-owned devices that connect to the Internet when outside the network and which are also used to access the Peralta District network must have a Host-based Firewall installed, appropriately configured and operating 24x7.
B. Users must not disable the Host-based Firewall software or otherwise prevent its proper operation.
C. Users must report Host-based Firewall alerts and or apparent malfunction to IT immediately.

2.3.3.5. Protecting Confidential Data in Transit

A. Confidential data must be protected in accordance with section 2.7.6 (Encryption) before being sent across public networks.
B. Systems that use keys or certificates for authentication or encryption must accept only trusted keys and/or certificates.
C. Protocols used to transmit confidential data across public networks must support only secure versions and configurations (e.g., only Secure Shell (SSHv2) a cryptographic network protocol).
D. Confidential data must not be sent via end-user messaging technologies (e.g.: e-mail, instant messaging type applications, etc.) unless it is appropriately encrypted in accordance with this policy.

2.3.3.6. Electronic Messaging Systems

A. Employees are informed of their responsibilities when using Peralta District -provided systems for email, voicemail, and the Internet.
B. Privacy of faculty, staff, and contractor email is not guaranteed.
C. All employees must acknowledge, that they understand their obligations to use email, voice mail, and the Internet in accordance with Peralta District policy (see AP 3720).

2.3.4. Encryption[27]

A. All encryption must meet the following requirements:
    1. Must use a strong, industry- and data-appropriate encryption algorithm (e.g.: Advanced Encryption Standard(AES))
    2. Encryption algorithm shall be configured to operate in a secure mode (e.g.: Offset Codebook Mode (OCB) an authenticated encryption mode of operation)
        a. Weak encryption algorithm modes such as the AES Electronic Code Book (ECB) mode must never be used.
    3. Encryption algorithm must use unique, randomly generated initialization vector values
    4. Strong key management practices (including unique & strong keys, key rotation, protection of keys, etc.) must be used to create and maintain the associated encryption keys.
B. All confidential data must be encrypted before being sent over a public network.
C. Confidential data must be encrypted in storage where feasible.
D. Confidential data should not be stored if it is not needed.
E. Where possible, confidential data should be stored as the result of a uniquely salted, random (one way) hash.
F. If confidential data cannot be stored as hash output, it must be encrypted per the above requirements.
G. It is recommended that employees use the encryption built into Microsoft outlook for any emails that contain private information. This encryption is offered on office 365 as well as all versions of Microsoft office from 2007 forward.

[27] NIST 800-53 SC-8 System and Communications Protection - https://nvd.nist.gov/800-53/Rev4/control/SC-8

2.3.5. Wireless Networking (Wi-Fi)[28]

2.3.5.1. Internal Wireless Network Requirements

A. Default SNMP community strings must be changed upon installation.
B. Default passwords/phrases on access points must be changed upon installation.
C. Other security-related wireless defaults must be changed.
D. Strong encryption must be used for Authentication over wireless networks.
E. Strong encryption must be used for Transmission over wireless networks.

2.3.5.2. Unauthorized Wireless Networks

A. The IT team is responsible for identifying unauthorized wireless networks.
B. The IT team must perform quarterly checks to detect and identify any unauthorized (and authorized) wireless access points for all system components and facilities, including at least the following:
    1. WLAN cards inserted into system components
    1. Portable or mobile devices attached to system components to create a wireless access point (e.g.: by USB, etc.)
    2. Wireless devices attached to a network port or network device
C. Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.

3. Software Development

3.1. Software Development Lifecycle

A. A rigorous Software Development Lifecycle (SDLC) helps to ensure consistency in development methodology and to provide secure, reliable and quality software development.
B. The Peralta Community College District must develop software in accordance with a documented, official Software Development Lifecycle.
C. The Software Development Lifecycle must document the following:
    A. Roles and responsibilities
    B. Change documentation
    C. Development of test plans
    D. Change testing and documentation of results
    E. Rollback plans
    F. Management review and approval
D. Alerts must be configured to monitor the source code in the Master branch to prevent unauthorized changes after passing QA testing and prior to deployment to production.

[28] NIST 800-53 AC-18 Wireless Access - https://nvd.nist.gov/800-53/Rev4/control/AC-18

3.2. Developer Access to Production

A. Peralta maintains a clear segregation of development and production environments. By default, developers do not have access to the production environment.

B. Access may be temporarily granted -- in accordance with the Access Request Procedure -- to a developer to troubleshoot an issue in the production environment. Once the issue is resolved the developer's access must be disabled.

C. In rare circumstances a developer may need long-term access to the production environment. Any such access must be documented in the approval ticket for that developer.

3.3. Third Party Library Code Review

A. Third party source code and license review is essential to ensure that all program code meets standards for quality, reliability, security, privacy and applicability, and that any Peralta development fulfills any applicable license obligations. The following process should be used to evaluate the inclusion of any vendor created source code:

1. Request to include new code
2. Review license(s)
3. Document license obligations, inform legal counsel if appropriate
4. Review technology for fit and security
5. Obtain approval to integrate from the STO

3.4. Secure Application Development

A. Software developed by any division of the Peralta Community College District must address common software vulnerabilities during the Software Development Lifecycle as follows:

1. Develop applications based on secure coding guidelines such as the OWASP Secure Coding Practices Quick Reference Guide.
2. Injection flaws are addressed by coding techniques that include:
    a. Validating input to verify user data cannot modify meaning of commands and queries.
    b. Using parameterized queries with bound variables.
3. Buffer overflows are addressed by coding techniques that include:
    a. Validating buffer boundaries.
    b. Truncating input strings.
4. Insecure cryptographic storage is addressed by coding techniques that:
    a. Prevent cryptographic flaws.
    b. Use strong cryptographic algorithms and keys.
5. Insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.
6. Improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details.
7. Coding techniques address any “high risk” vulnerabilities that could affect the application.
8. Cross-site scripting (XSS) is addressed by coding techniques that include

a. Validating all parameters before inclusion
b. Using context-sensitive escaping

9. Improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that includes:
    a. Proper authentication of users
    b. Sanitizing input
    c. Not exposing internal object references to users
    d. User interfaces that do not permit access to unauthorized functions
10. Cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.
11. Broken authentication and session management are addressed via coding techniques that commonly include:
    a. Flagging session tokens (for example cookies) as “secure”
    b. Not exposing session IDs in the URL
    c. Incorporating appropriate time-outs and rotation of session IDs after a successful login.

3.5. Development Data Sources

A. In order to maintain the Peralta Community College user’s privacy, Peralta develops its applications in an environment that does not contain the Peralta Community College user’s information.
B. Where necessary, Peralta may use a 'scrubbed' version of customer data such that all Confidential and Highly Restricted information is sufficiently masked, overwritten or removed prior to use for development or testing purposes.
C. Use of customer data for development or testing may be allowed in one of the following situations:
    1. When attempting to reproduce error conditions
    2. When benchmarking or other activities require a completely accurate representation of data
D. In the event that use of the Peralta Community College user’s data cannot be avoided, it must only be used in an isolated environment (e.g.: a separate VLAN) that has limited inbound network access and no outbound network access. Such data must be deleted as soon as practicable.

4. Data and Privacy Security

4.1. Data Classification

A. All data and media must be classified as public or confidential.

4.2. Public Data

A. Public data is information that may be open to the general public. Data classified as Public must not have existing local, national, or international legal restrictions on access or usage. Although security mechanisms are not needed to control disclosure and dissemination, they are still required to protect against unauthorized modification and destruction of information.

B. Examples of Public Data:
    1. Anything that has been officially made public by Peralta District (e.g.: blog posts, press releases)
    2. Distributed newsletter
    3. Official social media posts

C. Distribution of Public Data – Public Data may be distributed to the public by all employees at any time.

4.3. Confidential Data

A. Confidential data is information that must be secured due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statute requiring this protection. Confidential data may only be accessed by Peralta District employees, contractors, students, or partners who have a legitimate purpose for accessing such data.

B. Example of Confidential Data:

    Student, faculty and staff's personally identifiable information such as social security numbers, home addresses and other personal contact data.

C. Distribution of Confidential Data:

    Confidential information may only be accessible to parties who have a legal right to see the information. Confidential data must be appropriately protected (e.g.: by strong encryption and proper key management practices) while in storage or transit.

4.4. Intellectual Property Rights

A. Peralta District requires that all employees acknowledge their responsibilities via signature on a Confidentiality Agreement or Non-Disclosure Agreement (NDA) on their first day of employment. Additionally, Peralta District requires that all employees recognize the intellectual property rights of others via software copyright compliance practices.

4.5. Data Privacy

A. Peralta District understands that data privacy is an important issue for students, faculty and staff. The Peralta District Privacy Policy[29], prohibits sharing of student, faculty and staff data without consent except when under legal obligation.

B. Peralta District management must regularly inform employees of their obligations to adequately protect the data that Peralta District stores.

---

[29] http://web.peralta.edu/admissions/official-transcript-request/verificationsrelease-of-information/ferpa-2/

C. Peralta District reserves the right to routinely monitor employees' computer activities and communications in order to ensure compliance with the Privacy Policy and other applicable policies.

4.6. Data Confidentiality

A. Peralta District requires that access to confidential information be granted only after a confidentiality agreement is signed by the user and approved by the business unit related to the request (See PeopleSoft Security Access Request).
B. Only the Board of Trustees may approve changes to the Confidentiality Agreement Policy.
C. Confidential data must be protected during shipping and handling, electronic and physical transmission, and during storage and disposal.
D. All third parties to which Peralta District sends Confidential data must agree contractually to protect that data using commercially reasonable, industry-accepted measures that meet all applicable compliance requirements (e.g.: FERPA, HIPAA).

4.7. Masking of Sensitive Data

A. Confidential data must be appropriately masked where possible.
B. Masking of sensitive data must be done in an industry-accepted way and must comply with legal mandates and industry rules and regulations; for example:

    Credit card numbers should be masked such that only the last four digits are displayed where possible

C. Sensitive data should be removed from or masked in logs where possible.

4.8. Data Retention and Removal[30]

A. Storage of confidential data (e.g.: Social Security numbers, etc.) must be limited in amount and retention time to that which is required for legal and regulatory requirements.
B. Confidential data must be securely deleted or destroyed when no longer needed.
C. Legal and regulatory requirements for retention of all confidential data must be documented and that documentation must be retained for as long as it is applicable.
D. Physical media used to hold confidential data must be physically destroyed when it is no longer needed for business or legal reasons as follows:
    1. Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed
    2. Storage containers used for materials that are to be destroyed must be secured (e.g.: locked)
    3. Electronic media (e.g.: hard disk drives, DVD ROM discs, etc.) must be physically destroyed by a National Association for Information Destruction (NAID) certified vendor.

[30] NIST 800-53 MP-6 Media Protection - https://nvd.nist.gov/800-53/Rev4/control/MP-6

E. Physical media used to store confidential data must be securely wiped in accordance with DoD 5220.22 or NIST 800-88 standards before being repurposed. That media should still be physically destroyed when no longer needed.

4.9. Data Availability

A. All computers and communications equipment and all media must be protected from physical and environment hazards.
B. Peralta District must ensure that preventive maintenance of computer equipment occurs regularly.

4.10. Availability Monitoring

A. Availability-sensitive critical assets must be monitored be for production environment effectiveness, uptime and availability.
B. Availability monitoring systems must send appropriately prioritized alerts to authorized personnel when specified predefined thresholds are met.
C. Availability monitoring system alerts must be tracked and resolved in a timely manner:
    1. Critical severity alerts must be resolved as soon as possible
    2. High severity alerts must be resolved within 24 hours
    3. Medium severity alerts must be resolved within one month
D. Resolution of availability monitoring system alerts must be reviewed by management.

4.10.1. Backup Monitoring

A. Production environment backups must be monitored for failure using an automated system.
B. Failed production backups must result in an appropriately prioritized alert to authorized personnel.
C. Backup failure issues must be tracked and resolved in a timely manner.

4.11. Data Integrity

A. Data integrity is provided through Peralta District access and change control policies, application editing features, and related business policies and processes that secure resources against unauthorized modifications and allow changes to data and programs only via authorized personnel or processes, using established procedures.

5. Physical Security[31]

5.1. Building Access Control

A. Peralta must employ physical access controls to protect access to all buildings, such as proximity-based physical tokens (such as key Fobs) for larger buildings and key locks for smaller buildings.

[31] NIST 800-53 Physical and Environmental Protection - https://nvd.nist.gov/800-53/Rev4/family/PHYSICAL%20AND%20ENVIRONMENTAL%20PROTECTION

B. Employees and contractors are required to keep their Building Access Devices (e.g.: keys, proximity cards, etc.) with them at all times.
C. Building access must be approved by an authorized individual before they can be provisioned.
D. Building Access Devices (e.g.: keys, proximity cards, etc.) must be disabled and/or returned upon termination of an employee or contractor.
E. The Facilities team must perform quarterly reviews to ensure that all terminated employees have had Building Access Devices revoked.
F. Employees must lock desk drawers, cabinets and office doors when they leave their office.
G. Building entrance doors must remain locked at all times, with the exception of the main entrance doors. The doors at the main entrance may be unlocked during business hours if a receptionist is present and the main entrance doesn't provide immediate access to the rest of the building (e.g.: the main entrance leads to a lobby that is isolated from the rest of the building by locked doors).
H. Visitors should be easily identifiable (e.g.: by way of a 'visitor' badge).
I. Employees must lock up or destroy Confidential Data before leaving each day.
J. Peralta may perform periodic checks of employees' data storage and disposal practices via afterhours "desk checks" in order to ensure compliance with this policy.

5.2. Protection of Computer Equipment and Facilities

A. Physical access to data centers, server centers, Network Operations Centers (NOCs) and other key areas is restricted to authorized personnel.
B. All physical access to key areas must be recorded as an audit trail and the record must be maintained for at least three years.
C. Physical access audit trails must include the following:
    1. Name of person accessing the facility
    2. Campus/ Building name
    3. Location of access (e.g.: door number)
    4. Time of access
    5. Success or Failure attempt
    6. Employee ID number / Badge Number
D. Production computer and network equipment must be securely located in collocation facilities whose location is not advertised via signs or directories.
E. Collocation environmental protection mechanisms must include:
    1. Temperature and humidity monitors
    2. Preventive maintenance procedures
    3. Surge protection / power cleaning
    4. Backup power system
    5. 24x7 security guard presence

HIPAA Security Standards: Physical Safeguards - https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/physsafeguards.pdf?language=es

6. CCTV monitoring
7. Two Factor Authentication (2FA) for physical access

6. Incident Response Plan

6.1. Introduction

This Incident Response Plan is documented to provide a well-defined, organized approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the Peralta Community college district's private network. This Incident Response Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

This plan is designed to meet the following standards:

HIPAA/HITECH 164.308(a)(6), ISO/IEC 27001 A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2

6.2. Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team's mission is to prevent a serious loss of user confidence or information assets by providing an immediate, effective and skillful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Incident Response Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Director of Information Technology will coordinate these investigations.

6.3. Incident Response Team Members

President of the Board
Chancellor
Legal Counsel
College Presidents
Vice Chancellor of Finance
Vice Chancellor of Human Resources
Vice Chancellor of Educational Services
Vice Chancellor of Admissions and Records
Vice Chancellor of Information Technology

Director of Risk Management
Director of Network Services
Director of Enterprise Services
Public Information Officer

6.4. Incident Response Team Notification

For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the IT Department Help Desk will act as the central point of contact for reporting any incidents.

All computer security incidents reported to Help Desk must be reported to the Vice Chancellor of Information Technology. Simultaneously, a preliminary analysis of the incident will take place by the Director of Information Technology that will determine whether Incident Response Team activation is appropriate.

6.5. Types of Incidents

There are many types of computer incidents that may require Incident Response Team activation. Some examples include:

- Breach of personal information
- Denial of service/Distributed denial of service
- Excessive port scans
- Firewall breach
- Virus outbreak

6.6. Breach of Personal Information — Overview

This Incident Response Plan outlines steps our organization will take upon discovery of unauthorized access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a student, employee or client of Peralta.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the District collects about an individual is likely to be considered personal information if it can be attributed to an individual.

Personal information is defined as an individual's first name or first initial and last name, in combination with any of the following data:

- Social Security number
- Driver's license number or Identification Card number
- Financial account number, credit or debit card number
- Home address or e-mail address
- Medical or health information

6.7. Definitions of a Security Breach

A security breach is defined as unauthorized acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by Peralta. Good faith acquisition

of personal information by an employee, student or consultant for work related purposes is not a breach, provided that the personal information is not used or subject to further unauthorized disclosure.

6.8. Employee Responsibilities

All Peralta employees must report any suspected or confirmed breach of personal information on individuals to the IT Department immediately upon discovery. This includes notification received from any third-party service providers or other institutional agencies with whom Peralta shares personal information on individuals.

The employee reporting the suspected breach will assist in acquiring information, preserving evidence and providing additional assistance as deemed necessary by the Director of Information Technology or other Incident Response Team members throughout the investigation.

6.9. Classification / Identification of a Potential Incident

All reports of a potential incident shall be classified as a high/medium/low risk to facilitate the actions to take.

1. Criticality: High
    a. Definition: Incidents that have a monumental impact on Peralta's services, or potential liability, or impact Peralta's compliance with federal standards, to students, faculty and staff. Example: Unauthorized system access.
2. Criticality: Medium
    a. Definition: Incidents that have the potential to create a monumental impact on Peralta's services to students, faculty and staff.
        i. Example: Password cracking attempt.
3. Criticality: Low
    a. Definitions: Incidents that will minor impact on Peralta's services to students, faculty and staff.
        i. Example: Firewall scanning.

6.10. Response

Once a potential incident has been reported, the appropriate member of the IT Department should be notified for response. Members of the IT Department will be responsible for performing the initial investigation to determine if an incident has occurred. The following checklist identifies steps that can be used to facilitate in classifying the incident, if one in fact has occurred:

- Collection and review of log files
- Review of installed or running privileged programs
- Inspection for system file tampering
- Sniffer or Network Monitoring Programs reports
- Detection of unauthorized services installed on systems
- Evidence of password file changes

- Review system and network configurations
- Detection for unusual files
- Examination other hosts

Note: In responding to a reported incident, it may be good prudence to shut down any or all systems for the stopping of an attack in real time and/or the preservation of any potential forensic evidence.

6.11. Recovery

The main purpose of this Incident Response Program is to ensure an efficient recovery through the eradication of security vulnerabilities and the restoration of repaired systems. Recovery includes the ensuring the attacker's point of penetration and any associated vulnerabilities have been eliminated and all system operations have been restored.

6.12. Periodic Testing & Remediation

It is the responsibility of the IT Department to test and review the Incident Response Plan quarterly. When testing is done, each system should be scanned for the open vulnerability before remediation and then scanned again after the remediation to verify that the vulnerability has been eliminated.

6.13. Incident Response Plan Example

This document discusses the steps taken during an incident response plan**.**

1) Anyone who discovers the incident will contact the IT Help Desk. The Help Desk will log:
    a. Name of caller or source of incident alert (software notifications).
    b. Time of first report.
    c. Nature of the incident.
    d. What system(s) or persons were involved?
    e. Location of equipment or persons involved.
    f. How incident was detected.

2) The IT staff member who received the call will refer to their contact list for Incident Response Team to be contacted. The IT Help Desk will contact those designated on the list.
    The IT Help Desk will contact the IT Director using both email and phone messages. The IT Help Desk will log the information received. The IT Help Desk could possibly add the following information to the report:

    a. Is the equipment affected business critical?
    b. What is the severity of the potential impact?
    c. Name of systems being targeted, along with operating system, IP address, and location.
    d. IP address or any other information about the origins of the incident.

3) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

    a. Is the incident real or perceived?
    b. Is the incident still in progress?
    c. What data or property is threatened and how critical is it?
    d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
    e. What system or systems are targeted, where are they located physically and on the network?
    f. Is the incident inside the trusted network?
    g. Is the response urgent?
    h. Can the incident be quickly contained?
    i. Will the response alert the attacker and do we care?
    j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

4) An incident ticket will be created. The incident will be categorized into the highest applicable level of one of the following categories:

    a. High - Incidents that have a monumental impact on Peralta's services, or potential liability, or impact Peralta's compliance with federal standards, to students, faculty and staff.
    b. Medium - Incidents that have the potential to create a monumental impact on Peralta's services to students, faculty and staff.
    c. Low - Incidents that will minor impact on Peralta's services to students, faculty and staff.

5) Member of the IT Department will use investigative techniques, including reviewing of system logs, looking for gaps in logs, reviewing intrusion detection or firewall logs and interviewing witnesses to determine how the incident was caused. Only authorized personnel should be performing interview or examining IT systems. A chain of custody must be established and all potential evidence preserved and secured for turnover to proper authorities.

6) Incident Response Team will recommend changes to prevent the occurrence from happening again or spreading to other systems.

7) The IT Department will restore the affected system(s) to the pre-incident state and assess potential damages.

8) Post-mortem review of response and update policies – take preventive steps so the incident doesn't happen again.

   a. Would an additional policy have prevented the incident?

   b. Was a procedure or policy not followed which allowed the incident? What could be changed to ensure that the procedure or policy is followed in the future?

   c. Was the incident response appropriate? How could it be improved?

   d. Was every appropriate party informed in a timely manner?

   e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?

   f. Have changes been made to prevent another incident? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?

   g. Should any security policies be updated?

   h. What lessons have been learned from this experience?