IT Security for IT and Data Professionals Policy

Purpose and Scope

This policy outlines the responsibilities of IT and data professionals within [Client Name] ("[CI]"), and defines the specific controls required to secure the [CI] network, systems and data. It applies to all IT and Data Professionals working on [CI] systems, and all [CI] systems.

Responsibilities

Title or Role	What They are Responsible For
Chief Information Officer	Maintains and Enforces this policy.
IT and Data Professionals	Employees or contractors who have an elevated level of access to [CI] network or systems. These individuals have responsibility for selecting, purchasing, deploying, maintaining and/or disposing of [CI] network components, systems, or digital information, and have significant security responsibilities. Examples include network and system administrators, database administrators, and application administrators. These individuals have additional security responsibilities as outlined in this policy, and are responsible for implementing the detailed security controls required to protect the [CI] network, systems, and data.

Policy Statement

As outlined in IT Security Framework, different types of systems have different levels of security requirements. In the controls section of this document, the applicability of each control is identified based on the categorization of the system. Specifically, if a system does not meet the minimum definition of "Moderate" for Confidentiality, Integrity or Availability, certain controls are not required. This tailoring of the requirements for low security systems is based on the guidance in ***NIST 800-53 Rev 4***, ***Security and Privacy Controls for Federal Information Systems and Organizations.***

In this policy, we define the minimum expectations with respect to implementation of each security control – depending on the specific capabilities and limitations of each system, the exact way each control is satisfied may differ, and some systems may implement additional controls not specifically mentioned here. Exceptions to required security controls, e.g. because a specific technology cannot support it or it would be prohibitive to implement the control, will be evaluated based on risk, and must be approved by the Chief Information Technology Officer. Documentation of these exceptions and their rationale will be captured using Exhibit A, "Approval of IT Security Exception".

The security controls outlined in this document cover the full system life cycle. To avoid confusion, the controls are numbered consistently with the 14 security requirement families identified in **NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.**

These are: Table 1: Security Requirement Families

FAMILY	FAMILY
3.1 Access Control	3.8 Media Protection
3.2 Awareness and Training	3.9 Personnel Security
3.3 Audit and Accountability	3.10 Physical Protection
3.4 Configuration Management	3.11 Risk Assessment
3.5 Identification and Authentication	3.12 Security Assessment
3.6 Incident Response	3.13 System and Communications Protection
3.7 Maintenance	3.14 System and Information Integrity

In the Security Controls section below, each security requirement from the NIST 800-71 framework is listed, and the policy provides guidance on how [CI] systems shall satisfy that requirement. Controls that also satisfy other regulatory requirements (specifically PCI DSS), are specifically annotated. There is a cross-reference between the PCI DSS Requirements and the [CI] security controls in *IT Security Framework, IT Security Framework and Governance*.

To ensure clarity and simplify maintenance of the document, certain key components of this policy are broken out into separate documents. The numbering of these separate documents are consistent with their corresponding control family in **NIST Special Publication 800-171.** These include:

- IT Configuration Management– IT Configuration Management
- IT Security Incident Response – IT Security Incident Response

While many of the required security controls are the responsibility of IT professionals to implement and monitor, to fully protect [CI] confidential and internal data there are also specific requirements for end users and for 3rd parties who carry data on systems outside the [CI] network. These are broken out into separate policies, **End User Responsibilities, End User Responsibilities** and **IT Security for 3rd Party Partners & Providers, IT Security for 3rd Party Partners and Providers.** The organization of the guidance in these policies will follow the same general outline as the security requirement families above.

General Security Responsibilities of IT and Data Professionals

1. Select and implement systems that meet or exceed the security controls defined in this policy.
2. Manage security measures within the [CI] network and systems.
3. Conduct regular, randomized inspections of systems and network processes for security updates.
4. Maintain awareness of the evolving threat landscape, and initiate security and safety measures and strategies as necessary to adapt to new threats.
5. Customize access to information based on business needs and the data classification of the information. In general, access to all confidential information should be granted on a “need to know” basis, and access to all internal information should be restricted to [CI] employees and contractors with a need to know.
6. Maintain and update information security policies, procedures and services as required.

Security Controls

This section outlines the basic and derived security requirements as outlined in NIST 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, and how they are satisfied by [CI]. The requirements below sometimes refer to “Controlled Unclassified Information” (CUI) – within the [CI] data classification this is equivalent to Confidential data, and in general, includes all data categorized by the Family Educational Rights and Privacy Act (FERPA) as Protected data. Systems carrying only internal or public information are exempt from some of these requirements, and those exemptions are noted for each.

3.1 Access Control

Access control (AC) is the selective restriction of access to a system or resource. The act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization.

Basic Security Requirements:

3.1.1 Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

For new employees and contractors, access to specific systems will be granted based on their role within the organization. IT will maintain a set of standard profiles for different job functions to guide granting that access.

When an employee or contractor's job function changes, their access must be updated to match their new job profile, and permissions that are no longer required must be removed.

When an employee or contractor is terminated, their access must be terminated immediately. This is particularly important for employees who have elevated administrator privileges (generally IT and Data Professionals) and those who have access to Confidential data. In these cases, access should be revoked in parallel with the termination. For all other employees and contractors, access must be terminated the same business day as the termination.

All [CI] systems carrying internal or confidential information shall at a minimum require a username and password to access. Applications that are Active Directory aware (AD aware) can instead rely on the authentication done when logging into the end user workstation. In addition, accessing [CI] networks and systems from outside the network shall require two-factor authentication.

This control does not apply to systems that only carry public information, except for administrative functions.

3.1.2 Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

Controls 3.1.3-3.1.7 addresses how [CI] satisfies this requirement.
Derived Security Requirements:

3.1.3 Control the flow of confidential information in accordance with approved authorizations.

[CI] systems will only allow access or download of confidential information to users with a defined need-to-know based on their job role.

NOTE: This control also satisfies PCI Requirement #7, Restrict access to cardholder data by business need to know

3.1.4 Separate the duties of individuals to reduce the risk of malevolent activity without collusion.

Due to the relatively small size of the [CI] IT organization, separation of IT administrative duties is frequently not possible or required. However, all [CI] systems carrying confidential information, all financial systems, and all building security systems shall separate the IT administrative functions, such as account management, from the end user roles responsible for transactions.

3.1.5 Employ the principle of least privilege, including for specific security functions and privileged accounts.

All [CI] systems will use a "least privilege" approach and start with an initial "deny all" configuration, and use role-based security when possible. For systems carrying only public information, this will be limited to administrative functions. AD aware applications should implement this by leveraging synchronization with AD groups when possible. A role/responsibility matrix will be defined for all [CI] systems carrying confidential information, and revisited as part of the system upgrade process or when there is a change in organizational structure or responsibilities.

3.1.6 Use non-privileged accounts or roles when accessing non--security functions.

There will be separate dedicated system accounts for running automated tasks or running system or application services. [CI] IT professionals will maintain two accounts – one for normal office automation functions, such as e-mail or file access, and a separate one for administering systems and performing security functions. The following naming convention will delineate system, administrative, and end user accounts, when supported by the underlying technology:

1. System accounts will have prefix SYS
2. Administrative accounts will have a special, uniform prefix (such as A- or ADM-), followed by the IT professional's end-user account (e.g. A-smith or ADM-smith). The exact format used will depend upon the capabilities and limitations of each system, with the preferred format being the "ADM" prefix.
3. End-user accounts will not have a prefix.

3.1.7 Prevent non-privileged users from executing privileged functions and audit the execution of such functions.

Administrative privileges will only be granted to SYS or ADM accounts or where required for business-critical software or systems to function. Access logs will be maintained for all systems for a minimum of one month, and reviewed on a random basis or as required. All direct database access (queries) of any database containing confidential information is considered a privileged function.

File-integrity monitoring or change-detection software should be in place to prevent tampering with audit logs. New data added to logs should not cause an alert. *Note: This addresses PCI requirement 10.5.5.*

Audit logs should be retained for at least one year, with a minimum of 3 months immediately available for analysis (online or retrievable from backup within a few hours). *Note: This addresses PCI requirement 10.7.*

3.1.8 Limit unsuccessful logon attempts.

All non-system accounts will lock after 6 attempts, and stay locked for 30 minutes, or until unlocked by an administrator.

Note: This satisfies PCI Requirement 8.1.6 and 8.1.7.

3.1.9 Provide privacy and security notices consistent with applicable CUI rules.

When supported by the underlying technology, the following notice will be presented on the login screen for all systems or applications carrying confidential data. This same notice will be presented when logging into workstations or via VPN.

> **This is a [Client Name] ([CI]) system, and by logging in, you a) commit to following [CI] policy with regard to the handling of Internal and Confidential information, b) consent to monitoring, and c) explicitly recognize that you have no right to privacy with respect to your transactions on this system.**

3.1.10 Use session lock with pattern-hiding displays to prevent access/viewing of data after period of inactivity.

All [CI] workstations will lock after 15 minutes of inactivity, and use a screensaver that requires re-authentication once locked.

3.1.11 Terminate (automatically) a user session after a defined condition.

[CI] applications carrying Confidential information must terminate user sessions after 15 minutes of inactivity. This control is not required for systems that carry only Internal or Public information.

Note: This satisfies PCI Requirement 8.1.8.

3.1.12 Monitor and control remote access sessions.

The [CI] VPN solution will log all remote access sessions. These logs will be maintained for a minimum of one month, and will be subject to periodic review by the [CI] incident response team. The exception to this will be to [CI] cloud-based systems hosted outside the [CI] network. In those cases, the auditing mechanisms of the hosted solution will be used.

3.1.13 Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.

All remote access sessions will be encrypted using SSL 3.0 or an equivalent session encryption protocol.

3.1.14 Route remote access via managed access control points.

All remote access will be via the current [CI] VPN solution. The exception to this will be to [CI] cloud-based systems hosted outside the [CI] network. In those cases, the authentication mechanisms of the hosted solution will be used.

3.1.15 Authorize remote execution of privileged commands and remote access to security-relevant information.

All remote access will be via the current [CI] VPN solution and require two-factor authentication. The exception to this will be to [CI] cloud-based systems hosted outside the [CI] network. In those cases, the authentication mechanisms of the hosted solution will be used.

3.1.16 Authorize wireless access prior to allowing such connections.

Public wireless access without authentication may be allowed on a virtually segregated wireless network without access to [CI] systems and data. Students shall only be authorized to access wireless networks for academic, student-facing networks. Access to all other wireless networks is restricted to university employees and contractors.

3.1.17 Protect wireless access using authentication and encryption.

Access to the private [CI] wireless network that accesses [CI] applications will be authenticated using Active Directory (AD) credentials. All employee and contractor access will be encrypted using AES encryption.

3.1.18 Control connection of mobile devices.

Mobile access to the public wireless network, and the student network, will be allowed using an open access model, with limited constraints on type of traffic, except for pornography and other traffic that would violate acceptable use. Connection to the administrative networks require authentication. End User Responsibilities, End User Responsibilities, addresses the requirements and expectations of end users connecting mobile devices in more detail.

3.1.19 Encrypt CUI on mobile devices.

This is addressed in End User Responsibilities, End User Responsibilities, in the section on BYOD (Bring Your Own Device). It is an end user responsibility to ensure that any Confidential data stored on personal or mobile devices is encrypted.

3.1.20 Verify and control/limit connections to and use of external information systems.

A firewall is required at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.

Only port 80 and port 443 (unencrypted and encrypted web traffic) are allowed through the firewall by default. All other outbound connections must be granted via specific firewall rules, and limited to known IP addresses or IP address ranges.

NOTE: This control also addresses in part PCI DSS Requirement #1, Install and Maintain a Firewall Configuration to Protect Cardholder Data

3.1.21 Limit use of organizational portable storage devices on external information systems.

This will be addressed in End User Responsibilities, End User Responsibilities, and addressed in End User training (see section 3.2, Awareness and Training).

3.1.22 Control information posted or processed on publicly accessible information systems.

MU Internal and Confidential data shall not be posted or processed on public information systems.   The Director, Marketing and the CIO have responsibility for monitoring compliance with this policy.

3.2 Awareness and Training

Basic Security Requirements:

3.2.1 Ensure that managers, systems administrators, and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems.

End user responsibilities, and end user security awareness training, are addressed in End User Responsibilities, End User Responsibilities. *Note: this addresses PCI requirement 12.6.*

All IT and Data Professionals, including contractors, will be required to review this policy within 60 days of joining the organization, and before being granted system administrative privileges. Existing faculty and staff will be notified each time this policy is revised, and be required to acknowledge within 30 days after the update is published.

Acknowledgement of review and acceptance of this policy will be accomplished by e-mail, using the language in Exhibit B, "Acknowledgement of Review of IT 3.0". This e-mail must be sent to the Chief Information Technology Officer or his designee, and will be stored in a secure central location.

3.2.2 Ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

In addition to the policy review outlined in section 3.2.1, all employees within the IT organization must participate in at least 8 hours of additional IT security training annually. This training may come in the form of face-to-face training, webinars, or other modalities. The specific security training will be reviewed and approved by the Chief Information Technology Officer, and each team member will maintain a log of their training activities in a central location.

Derived Security Requirements:

3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.

At least one hour of the training in section 3.2.2 must be on recognizing and reporting indicators of insider threat.

3.3 Audit and Accountability

Basic Security Requirements:

3.3.1 Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.

See specific guidance in the derived security requirements below.

3.3.2 Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Whenever supported by the underlying technology, entries in all audit logs shall be correlated to the Active Directory user ID. If that is not possible, the user id for the specific system shall be used, if applicable. *NOTE: This control satisfies in part PCI DSS Requirement #10, Track and monitor all access to network resources and cardholder data*.

Derived Security Requirements:

3.3.3 Review and update audited events.

[CI] is working toward a centralized monitoring solution that will be used for reviewing and correlating auditable events. A Security Information and Event Management solution (SIEM) will be evaluated at a future date. Until those systems are in place, review of audited events is done manually, triggered by a suspected security incident, as described in IT Security Incident Response.

3.3.4 Alert in the event of an audit process failure.

Standard system images will be defined that will cause processing to halt in the event space is exhausted for the audit log. Monitoring will be put in place to alert if audit logs do not change within expected timeframes (exact timeframe will be defined based on the system being monitored.

3.3.5 Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

In the event of a potential security incident, a “war room” is created. The network administrators and other key staff on the incident response team coordinate investigation of logs at different levels of the architecture. As the investigation proceeds, the incident response team will do manual correlation of events as part of the investigative process. See IT Security Incident Response.

3.3.6 Provide audit reduction and report generation to support on-demand analysis and reporting.

This is currently addressed manually in the war room approach addressed in 3.3.5 above. [CI] will evaluate implementation of a SIEM at a future date.

3.3.7 Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.

[CI] uses the NTP (Network Time Protocol) to maintain accurate time on all servers, workstations and network devices. All devices will either synchronize with the NIST Internet time service, or with one of the internal NTP servers which in turn synchronize with the NIST Internet time service.

3.3.8 Protect audit information and audit tools from unauthorized access, modification, and deletion.

Audit logs will be stored on file shares with access limited to essential personnel and backed up along with all other business data.

All 3rd party audit tools will be installed in file shares with access limited to IT security personnel, and run using dedicated system accounts.

Server logs and network logs will be protected in accordance with best practice guidelines from their respective vendors.

3.3.9 Limit management of audit functionality to a subset of privileged users.

Only permanent members of the incident response team (see IT Security Incident Response) will have access to audit functionality and audit logs from security devices. This will be enforced via membership in the “InfoSec” AD group. Normal server and workstation logs will be restricted to those members of the IT team with administrative privileges.

3.4 Configuration Management

See separate policy IT Configuration Management.

NOTE: IT Configuration Management controls also partially satisfy PCI Requirement #6, Develop and maintain secure systems and applications. Since [CI] does not develop its own systems, the remainder of this PCI requirement is addressed in IT Security for 3rd Party Partners & Providers, IT Security for 3rd Party Partners and Providers, which addresses selection and contracting of 3rd party software.

3.5 Identification and Authentication

Basic Security Requirements:

3.5.1 Identify information system users, processes acting on behalf of users, or devices.

All users will be assigned unique identifiers. Group (shared) accounts are prohibited. Whenever possible, systems will rely on the underlying Active Director (AD) user account for identification. See section 3.1.6 for specific requirements for system and administrative accounts.

NOTE: This control satisfies PCI requirement #8, Assign a unique ID to each person with computer access, and more specifically addresses PCI 8.5.

3.5.2 Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

All users must authenticate to [CI] systems and applications. Specific username and password requirements are addressed in the derived security requirements below.

Derived Security Requirements:

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Two-factor authentication is required for VPN access to the [CI] network, and for login to all administrative accounts (as defined in section 3.1.6), where supported by the underlying technology.

Note: addresses PCI requirement 8.3.1

3.5.4 Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

[CI] relies on the login features of the underlying operating systems for servers, workstations and network devices to satisfy this requirement. The group policy object for all [CI] devices will prevent storage of credentials or .NET passports for network authentication.

3.5.5 Prevent reuse of identifiers for a defined period.

User accounts will be disabled, not deleted, for a period of one year. This prevents reuse of identifiers, and also ensures that security log entries can be traced to specific users (see section 3.3.2 above)

3.5.6 Disable identifiers after a defined period of inactivity.

Standard employee and contractor accounts are typically disabled within hours of termination, but always within 24 hours.

A script will be run at least monthly to disable accounts that have been inactive for over 90 days.

Note: this addresses PCI requirement 8.1.4, which requires disabling inactive accounts after 90 days.

Third parties that have user IDs on [CI] systems that are used for maintenance purposes must be disabled whenever not in use, and must be audited in the same way as all privileged account activity. The exception to this would be accounts that are used on an ongoing basis (e.g. managed services used for remote monitoring) as part of normal operations.

Note: this addresses PCI requirement 8.1.5.

3.5.7 Enforce a minimum password complexity and change of characters when new passwords are created.

Passwords must be a minimum of 8 characters long, and must contain at least one of each of the following:

- Upper case letter (A-Z)
- Lower case letters (a-z)
- Numbers (0-9)
- Special characters (e.g. !, #, &, %, extended ASCII, etc.)

Group policies will be used to enforce this, and also that passwords must be changed after first created. All systems must have a mechanism for verifying user identity before modifying user account names or passwords. The mechanism may be different depending on system and circumstance—security questions, IT team confirmation of identity directly, etc.

Note: addresses PCI requirement 8.2.2 and 8.2.3.

3.5.8 Prohibit password reuse for a specified number of generations.

The Enforce Password History setting will be set in Group policies to prevent user passwords from being the same as the last 6 passwords used. End user passwords for all systems and applications must expire within 180 days of assignment. The exception are user accounts used in executing automated functions (service accounts) – these may be set to never expire, but must also be defined to prevent direct login. The definition of service accounts would include any database accounts used by applications to access the database.

3.5.9 Allow temporary password use for system logons with an immediate change to a permanent password.

The temporary password when creating new accounts for [CI] systems will be assigned by the IT team member who creates the account.

Note: addresses PCI requirement 8.2.

3.5.10 Store and transmit only encrypted representation of passwords.

The built-in capabilities of the server, workstation and network device operating systems will be used to enforce this requirement. If a centralized password vault is used to store system account passwords, it will be encrypted using AES-256 encryption and the password for the vault will follow the same password complexity requirements as all other passwords. All [CI] 3rd party applications must enforce encryption of passwords at rest. Web-based systems must use https for the login process.

Note: addresses PCI requirement 8.2.1.

3.5.11 Obscure feedback of authentication information.

Passwords should be masked and not displayed on screen. This is built-in to Windows and most applications.

3.6 Incident Response

See separate policy IT Security Incident Response, IT Security Incident Response

3.7 Maintenance

Basic Security Requirements:

3.7.1 Perform maintenance on organizational information systems.

Standard practice will be to maintain all 3rd party software within one major revision of the latest available. Software patches on operating systems and applications will be reviewed and applied at least monthly, with security patches applied more frequently based on the criticality of the vulnerability being addressed and the system being patched. Additional details are contained in Configuration Management.

3.7.2 Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

Server and network device patches will only be applied by authorized IT professionals. Patches will be downloaded from known sources, and if stored within the [CI] network, on file shares with access restricted to authorized IT team members. Workstation patches may be applied by either IT team members or end users, depending upon specific circumstance and assessment of risk.

Derived Security Requirements:

3.7.3 Ensure equipment removed for off-site maintenance is sanitized of any CUI.

All equipment must be sanitized when removed for maintenance using a method consistent with NIST 800-88, Guidelines for Media Sanitization. This policy will not apply to support organizations that demonstrate equivalent controls or superior controls to those contained here, and whose contract includes explicit requirements to protect [CI] data and systems. IT Security for 3rd Party Partners and Providers, provides more detail on what is required. This includes offsite backup storage providers, who must meet the same requirements.

3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

All media containing diagnostic and test programs will go through standard anti-virus scans. University-wide AV policies will scan all media immediately when connected to the system.

3.7.5 Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

All remote connections will use standard two-factor authentication to establish VPN connections. IT professionals and 3rd party contractors shall terminate their VPN session as soon as maintenance is complete. VPN connections will automatically disconnect after 30 minutes of inactivity. Also – see section 3.5.6, which requires that 3rd party maintenance accounts be disabled when not in use and monitored when in use.

Note: addresses PCI requirement 8.3.

3.7.6 Supervise the maintenance activities of maintenance personnel without required access authorization.

3rd party contractors performing maintenance will be escorted while on site, and their entry and exit must be logged.

3.8 Media Protection

Basic Security Requirements:

3.8.1 Protect (i.e., physically control and securely store) information system media containing CUI, both paper and digital.

All systems and media containing Confidential data must be kept in a room that is locked when not in use. Whenever feasible, Confidential data should not be stored on laptops or other mobile devices. Confidential data should be encrypted at rest. The preferred method to ensure this is whole disk encryption. All card reading equipment surfaces must be inspected at least annually to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).

Note: Examples of signs that a device might have been tampered with or substituted include unexpected attachments or cables plugged into the device, missing or changed security labels, broken or differently colored casing, or changes to the serial number or other external markings.

NOTE: This control satisfies PCI Requirement #9, Restrict physical access to cardholder data, and specifically requirement 9.9.2, which deals with detecting device tampering, and 12.6, which requires general security training with respect to processing payment cards.

3.8.2 Limit access to CUI on information system media to authorized users.

All file shares containing confidential information will have access limited to specific AD groups with a job requirement to access the data.

3.8.3 Sanitize or destroy information system media containing CUI before disposal or release for reuse.

All media disposed of shall be sanitized using a method consistent with NIST SP 800-88, Guidelines for Media Sanitization.

Derived Security Requirements:

3.8.4 Mark media with necessary CUI markings and distribution limitations.

Backup and other removable media shall be marked "[CI] Confidential." Font size will be at least 12-point Times Roman when practical, or the largest size possible where not.

3.8.5 Control access to media containing CUI and maintain accountability for media during transport outside of controlled areas.

A log shall be maintained in a central location of confidential data being transported outside of normal backup and recovery or other standard business processes that require transport of confidential data. Logging and tracking requirements must be incorporated into standard operating procedures for ongoing transfers of confidential data.

3.8.6 Implement cryptographic mechanisms to protect the confidentiality of CUI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

All electronic Confidential data shall be encrypted at rest and in transport. Any exceptions must be addressed as a policy exception and explicitly authorized as such.

3.8.7 Control the use of removable media on information system components.

Only [CI] owned removable media should be attached to [CI] systems. Removable media containing Confidential data should be encrypted, when possible, and when not, the data itself must be encrypted.

3.8.8 Prohibit the use of portable storage devices when such devices have no identifiable owner.

Addressed in 3.8.7.

3.8.9 Protect the confidentiality of backup CUI at storage locations.

Addressed in 3.7.3, 3.8.4 and 3.8.5.

3.9 Personnel Security

Basic Security Requirements:

3.9.1 Screen individuals prior to authorizing access to information systems containing CUI.

All IT and Data Professionals must undergo a standard background check as part of the hiring process, in addition to the evaluation of their competencies by evaluating their resume, during interviews and via reference checks. 3rd party contractors should also be evaluated, with the level of evaluation dependent upon the organization and the length of the relationship with [CI].

3.9.2 Ensure that CUI and information systems containing CUI are protected during and after personnel actions such as terminations and transfers.

Account access for IT and Data Professionals and others with access to Confidential data must be terminated immediately upon termination.

Derived Security Requirements: None.

3.10 Physical Protection

Basic Security Requirements:

3.10.1 Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

All storage systems, network equipment and servers carrying confidential data must reside in a locked data center with access logged, and limited to the IT team and other personnel with a bona fide job requirement to access. This includes systems hosted by 3rd parties that carry [CI] data, and will be addressed in IT Security for 3rd Party Partners & Providers.

3.10.2 Protect and monitor the physical facility and support infrastructure for those information systems.

Data centers must meet the following minimum requirements, and these requirements must be formally reviewed annually.

Power – conditioned power with UPS battery backup. Alternative power (e.g. diesel generators) that provide power for up to 24 hours in the event of a power outage are preferred. Power monitoring should be in place.

Network – a redundant network architecture that minimizes single points of failure. Network monitoring should be in place.

Servers – servers (or virtual server farms) supporting medium availability systems should have a fault-tolerant configuration (redundant servers, dual NICs, RAID drives, etc).

Cooling – adequate air conditioning should be in place to avoid damage to equipment. Temperature and humidity monitoring should be in place, and kept within industry standard norms. Standard practice here continues to evolve, but currently are 68 – 75 Fahrenheit, with humidity between 45-55%. Alternate cooling designs that provide a satisfactory operating environment for equipment are also acceptable.

Fire detection & suppression - Heat and smoke detectors should be in place and monitored, and a fire suppression system appropriate for computer data centers.

Physical security – **video monitoring** should be in place, as well as electronic access control and logging. If the equipment is in a multi-tenant data center, [CI] equipment should be in locked racks. There should be appropriate building security in place as well that controls access to the area the data center is in.

Derived Security Requirements:

3.10.3 Escort visitors and monitor visitor activity.

All visitors to [CI] data centers (including 3rd party data centers and data centers supporting hosted systems) must be escorted.

3.10.4 Maintain audit logs of physical access.

The logs of data center access should be retained for a minimum of 6 months.

3.10.5 Control and manage physical access devices.

Systems and devices that control physical access (such as door lock systems) must meet the same standards of protection as systems carrying Confidential data.

3.10.6 Enforce safeguarding measures for CUI at alternate work sites (e.g., telework sites).

Employee responsibilities when accessing Confidential data from personal devices (at home or elsewhere) are addressed in End User Responsibilities. All access to [CI] systems is subject to monitoring and will be logged (see 3.1.14).

3.11 Risk Assessment

Basic Security Requirements:

3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.

The Chief Information Technology Officer will conduct a bi-annual risk assessment and provide a summary of that assessment to the President and his Cabinet. This assessment will detail the major networks and systems used by [CI] (including 3rd party hosted systems), assess their compliance with this policy, and discuss the residual risk to [CI]'s mission, business functions, image and reputation.

Derived Security Requirements:

3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.

1) A quarterly 3rd party vulnerability scan will be done on [CI]'s network and systems, including an external penetration test. This must be done by an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved.
2) Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC).
3) Internal scans are done on an ongoing basis for open ports and other vulnerabilities.
4) External and Internal scans will be done as necessary based on security incidents, new information on potential vulnerabilities and after major system changes. This is reflected in Configuration Management.
5) The Incident Response Team will monitor available national databases of vulnerabilities, and define action plans for Critical and High rated vulnerabilities relevant to [CI]'s infrastructure. There are several specific feeds monitored, including:
   a. The Head of Security gets a periodic update from the FBI Cybercrimes unit flagging new threats. This information is used by the Incident Response team to guide emergency patching for critical vulnerabilities.

b. Product vulnerability notifications. These include notifications from Microsoft, Apple and Cisco.

3.11.3 Remediate vulnerabilities in accordance with assessments of risk.

Critical vulnerabilities from NVD that are relevant to [CI]'s systems should be remediated (typically by patching) within one week, or faster depending upon the vulnerability and the level of risk to [CI] operations. High vulnerabilities should be remediated within one month, and within the normal patching cycle whenever possible. Medium and Low vulnerabilities will generally be remediated during the normal patch cycle.

Vulnerabilities identified during 3rd party and internal scans, or during incident response handling, will have an action plan defined and timing for remediation should be consistent with NVD identified vulnerabilities.

3.12 Security Assessment

Basic Security Requirements:

3.12.1 Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.

This policy will be reviewed at least every two years against current best practices and updated as appropriate. [CI]'s policy and procedures will also evolve based on the lessons learned from security incident handling (see IT Security Incident Response).

3.12.2 Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.

The incident response team (see IT Security Incident Response) will create an action plan with target dates to address specific vulnerabilities identified during external or internal assessments, critical vulnerabilities, or action items stemming from lessons learned sessions during the incident handling process. Medium and low vulnerabilities will generally be addressed during the normal patching cycle or as part of normal maintenance.

3.12.3 Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

A random sampling of systems will be assessed on an annual basis to evaluate the effectiveness and consistency of application of the controls defined herein.

NOTE: This control satisfies PCI Requirement #11, Regularly Test Security Systems and Processes.

Derived Security Requirements: None.

3.13 System and Communications Protection

Basic Security Requirements:

3.13.1 Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

Firewalls shall be in place between the public Internet and all [CI] systems carrying Internal and Confidential data. The firewall shall be configured taking a "deny all" approach, opening up the minimum of ports and external IP address ranges required to support business operations. The exception to this is the public WIFI and any event network, which allows all ports and addresses.

Firewalls and routers must be configured to:

1) Only allow “established” connections
2) Prevent unauthorized outbound traffic to the Internet
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) Prevent unauthorized traffic between the public wireless environment and the internal network

NOTE: This control also addresses in part PCI DSS Requirement #1, Install and Maintain a Firewall Configuration to Protect Cardholder Data and PCI DSS Requirement #10, Track and monitor all access to network resources and cardholder data.

3.13.2 Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

[CI] takes a defense-in-depth approach to security, including:

1) Perimeter security (firewalls and Intrusion Prevention Systems)
2) Server hardening, patching and vulnerability management
3) AV protection
4) Role-based security for file shares and applications
5) A “least privilege”, “deny all” approach to system configuration that limits access to the minimum required to support business operations.

[CI] does not develop software internally, so the issue of security review in the SDLC does not apply.

NOTE: The server hardening part of this control must also include satisfying PCI DSS Requirement #2, Do not use vendor-supplied defaults for system passwords and other security parameters.

<u>Derived Security Requirements</u>:

3.13.3 Separate user functionality from information system management functionality.

All [CI] systems and applications must have separate roles and access defined for administrative access from end users. [CI] maintains a dedicated IT function that has primary responsibility for administrative functions. Business users outside IT may perform some application-specific administrative roles (e.g. Colleague administration).

3.13.4 Prevent unauthorized and unintended information transfer via shared system resources.

This is minimized by taking a role-based view to security, and using Active Directory OU groups to limit access to shared file shares. Cloud-based file share controls are generally maintained by the end user responsible for that content.

3.13.5 Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

[CI] maintains VLANS for different functions. There is one VLAN for administrative systems, one for academic systems, one for Security, one for any card-swipe devices, one for student access, and potentially public WIFI VLANs. VLANs will not be routable to each other unless explicitly required for a valid university application.

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

The external firewalls will be configured using a deny all base configuration, then selectively opening ports and IP address ranges.

Known malicious sites will be blocked at the firewall level. Additional application filtering may be put in place as well. End user guidance on appropriate Internet Usage will be addressed in End User Responsibilities.

3.13.7 Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.

Split-Tunneling will be prohibited by the firewall and VPN solution.

3.13.8 Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards.

All Confidential data must be encrypted in transit. Confidential data accessed via Web-based systems (whether internal or external to the [CI] network) must use https, with the latest TLS encryption version (currently TLS 1.2). Confidential data transmitted via e-mail must be encrypted in a file attachment (e.g. password protection of a Microsoft Office document), the password must meet password complexity requirements outlined in 3.5.7, and the password must be passed either verbally or in a separate e-mail. If files are passed via FTP, secure FTP must be used or they should be encrypted in the same way as when sending via e-mail. Files passed via a cloud-based file service, such as DropBox, OneDrive, or Box should use the features of those systems for encryption, or they should be encrypted at the file level in the same way as when passed via e-mail.

NOTE: This control also satisfies PCI DSS Requirement #4, Encrypt transmission of cardholder data across open, public networks.

3.13.9 Terminate network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

Group policies will be defined to terminate RDP (Remote Desktop Protocol) sessions after 30 minutes of inactivity. VPN sessions will follow the same protocol. The firewall will be configured to terminate “dead peer connections”.

Note: This addresses PCI requirement 12.3.8.

3.13.10 Establish and manage cryptographic keys for cryptography employed in the information system.

Standard certificate authorities will be used to establish certificates used on all [CI] systems.

3.13.11 Employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

Data stored at rest should be encrypted using AES 256 whenever possible. Standard Microsoft Office encryption is AES 128 – this is acceptable for temporary storage and transfers of small amounts of confidential data, but for transfer of large amounts of data, Files should be zipped and encrypted using AES 256. For web-based systems,TLS 1.2 encryption should be used, using AES 256 cipher settings.

NOTE: This control also satisfies PCI DSS Requirement #3, Protect stored cardholder data.

3.13.12 Prohibit remote activation of collaborative computing devices and provide indication of devices in use to users present at the device.

Remote activation of collaborative computing devices will be disabled when supported by the underlying technology. Indication of when the devices are in use will be implemented if supported by the underlying technology.

3.13.13 Control and monitor the use of mobile code.

[CI] will use code reviews as necessary to ensure that mobile code is not introduced on its publicly facing websites. This requirement will be addressed in IT Security for 3rd Party Partners & Providers for 3rd party partners and providers of IT services.

3.13.14 Control and monitor the use of Voice over Internet Protocol (VoIP) technologies.

The IT team will monitor VOIP traffic in the same way as all other network traffic, and take action if it materially interferes with the availability of systems or networks.

3.13.15 Protect the authenticity of communications sessions.

Web-based systems will use standard session maintenance to protect the authenticity of communication sessions, and shall invalidate session identifiers when the session is terminated. As [CI] does not develop its own software, this will be addressed in IT Security for 3rd Party Partners & Providers.

3.13.16 Protect the confidentiality of CUI at rest.

This is addressed in 3.13.11. FIPS-validated cryptography shall be used both when Confidential data is in transit and at rest.

3.14 System and Information Integrity

Basic Security Requirements:

3.14.1 Identify, report, and correct information and information system flaws in a timely manner.

This is addressed in section 3.4 and 3.12 for security related flaws. Information flaws (incorrect information) will be managed via normal operating processes, and for financial information, as part of the normal financial controls. Defects in software provided to [CI] by vendors will be addressed on a case-by-case basis with the vendor, and generally addressed via software maintenance, as addressed in Configuration Management.

3.14.2 Provide protection from malicious code at appropriate locations within organizational information systems.

Anti-virus software will be installed and maintained up-to-date on all [CI] servers and workstations.

3.14.3 Monitor information system security alerts and advisories and take appropriate actions in response.

This is addressed in section 3.11.2.

NOTE: These controls also satisfy PCI Requirement #5, Use and regularly update anti-virus software or programs.

Derived Security Requirements:

3.14.4 Update malicious code protection mechanisms when new releases are available.

When possible Intrusion Prevention System (IPS) and anti-virus systems will be set to update automatically from the vendor. IPS and Anti-virus software will be given priority during the normal system maintenance and patch cycles, as addressed in IT Configuration Management.

3.14.5 Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Anti-virus software will be configured to scan all removable media as soon as it is connected to the device. It will also be configured to do full scans nightly during off-hours on all servers and workstations.

3.14.6 Monitor the information system including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

An Intrusion Prevention System shall be in place for all [CI] connections to the public Internet.

3.14.7 Identify unauthorized use of the information system.

This will be addressed through use of the IPS, and via the security incident response mechanisms outlined in IT Security Incident Response.

References

This section contains any 3rd party standards, guidelines, or other policies referenced by this policy.

1. **NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,** National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
2. **NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,** National Institute of Standards and Technology, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
3. **NIST National Checklist Program Repository,** https://web.nvd.nist.gov/view/ncp/repository
4. **SANS Institute InfoSec Reading Room, Detecting and Preventing Unauthorized Outbound Traffic,** https://www.sans.org/reading-room/whitepapers/detection/detecting-preventing-unauthorized-outbound-traffic-1951
5. A Practical Methodology for Implementing a Patch management Process, https://www.sans.org/reading-room/whitepapers/bestprac/practical-methodology-implementing-patch-management-process-1206

6. NIST 800-88, Guidelines for Media Sanitization, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
7. Payment Card Industry (PCI) Data Security Standard, v3.2

Exhibits

This section contains links to any documents that are required to be used by the policy. Examples would include required forms or links to internal websites or systems required to implement the policy.

Exhibit A	Approval of IT Policy Exception
Exhibit B	Acknowledgement of Review of IT Security for IT and Data Professionals
Exhibit C	

Exhibit A – Approval of IT Policy Exception

Requestor:	
Date Requested:	*Date of request. The approval date is below in the signature section*
Policy reference:	*Specific policy section to which an exception is being requested*
Description of systems or applications impacted:	
Rationale for the exception:	*Options may include lack of support from underlying technology. If there are any compensating controls, these should be noted here.*
Business Risk:	*A discussion of the potential impact to confidentiality, integrity or availability of the systems or applications goes here.*
Approved By:	
Title:	*Per policy, this should always be the Chief Information Technology Officer*
Date Approved:	

Exhibit B - Acknowledgement of Review of IT Security for IT and Data Professionals

The language below shall be used to acknowledge review and acceptance of the IT 3.0 policy by IT and Data Professionals.

> Subject: Acknowledgement of Review IT Security for IT and Data Professionals
>
> I acknowledge that I have reviewed **IT Security for IT and Data Professionals**, understand my responsibilities as outlined therein, and agree to comply to the best of my ability. I also understand that failure to comply with [CI] security policies may result in disciplinary action.

Procedures

N/A

Related Policies

- **Acceptable Use**
- **Asset Management**

- **IT Security Framework**
- **End User Responsibilities**
- **IT Security for IT and Data Professionals**
- **IT Configuration Management**
- **IT Security Incident Response**
- **IT Security for 3rd Party Partners & Providers**
- **Web Accessibility Policy**

History of the Policy

2022-12-20 – The President of the University approved the establishment of this policy upon recommendation of the President's Cabinet.

MARYWOOD UNIVERSITY
POLICIES AND PROCEDURES MANUAL