The Pennsylvania State University
College of the Liberal Arts

Information Technology Security Policy Manual

Owners: IT Management Team
Veronica Longnecker – IT Director
Greg Giles - Web and Infrastructure and Enterprise Team Manager
Travis Freehauf - Web Technologies Team Manager
Art Fogleman - Service and Support Team Manager

Authorized Users: Liberal Arts Faculty, Staff, Graduate Student, Undergraduate Student, and

any other person given access to use a Liberal Arts-owned computing resource.

NOTICE TO HOLDERS OF PAPER COPIES: Please verify that this document is still current. Upon receipt of a new issue, destroy the previous issue.

This document should be shredded upon the end of its use.

Table of Contents

Executive Summary

This Information Technology Security Policy Manual describes the security policy statements that govern the security performance and concerns of the College of the Liberal Arts in terms of intranet, local network, extranet, key servers, and desktop computing devices in conjunction with the information contained on such networks and devices. The security policy statements contained in this document will be satisfied by execution of security policy enforcement mechanisms that will be implemented by automated or manual means. Actual implementation strategies, countermeasures, and security procedures will be the focus of supporting procedures and guideline documents.

The purpose of this policy manual is to ensure the development and implementation of cost effective controls that prevent the unauthorized access, modification, destruction, or disclosure of College data at any level and to provide the ability to recover information or information processing capabilities.

This policy is deemed critical for the College of the Liberal Arts information asset protection.

Information Security Documentation

Scope

The scope for the security policy manual and all policies listed herein applies to all information processed, stored, and transmitted by the College of the Liberal Arts. The policies set forth in this document also apply to interfaces with other University entities and second- or third-party partners who connect to the Liberal Arts networks and systems hosted at the Pennsylvania State University, College of the Liberal Arts, University Park main campus facilities and any Liberal Arts-owned computing resources housed off-campus.

Purpose

The purpose of this document is to provide Liberal Arts employees and users with specific guidelines to follow with respect to information security and assurance.

References to Existing Documentation

The following documents have been referenced in part in this security policy:

The Pennsylvania State University Administrative Policies

AD19 – Use of Penn State Identification Numbers and Social Security Number
AD20 – Computer and Network Security
AD22 – Health Insurance Portability and Accountability Act (HIPAA)
AD23 – Use of Institutional Data
AD35 – University Archives and Records Management
General Retention Schedule
AD53 – Privacy Statement
AD54 – Web Page Design and Image
ADG02 - Computer Facility Security Guidelines
AD71 – Data Categorization
FN21 – Non-Office Telecommunications Services

Pennsylvania State Law

Pennsylvania Breach of Personal Information Notification Act

The College of the Liberal Arts Policies and Agreements

Information Technology Security Policy Manual
Information Technology Security Policies User Agreement
Personally Identifiable Information User Agreement

Acronyms Used Throughout this Document

CLA – College of the Liberal Arts
HIPAA – Health Insurance Portability and Accountability Act
PII – Personally Identifiable Information (such as Social Security number, credit card number)

Definitions

- **AES-128 algorithm standard –** Advanced Encryption Standard (AES) is a cryptographic algorithm that can be used to protect electronic data. The AES algorithm symmetric-key block cypher that can encrypt (encipher) and decrypt (decipher) information. The 128 represents the number of bits of the cryptographic key to encrypt and decrypt data in blocks of 128 bits.
- **CLA Networks –** College of the Liberal Arts network infrastructure both wired and wireless for network connectivity to online resources including, but not limited to the Internet, Intranet, College of the Liberal Arts servers and services, and University servers and services.
- **College of the Liberal Arts/University owned computing resource** – University owned equipment includes, but is not limited to, equipment purchased with general department funds, grants (federal, state, foundation, company), startup funds, research account funds, or any funds originating from Penn State. University owned equipment also includes any equipment purchased from another institution/entity via a grant, but which has since been transferred to Penn State.
- **Compromise** - When unauthorized access to a computing resource has occurred, or has a high probability of having occurred.
- **Department of Defense (DoD) Sanitization Standard** - a software based data sanitization method (typically referred to as DoD 5220.22-M) used in various data destruction programs to overwrite existing information on a hard drive or other storage device to render the data unrecoverable.
- **Employee** – Refers to all full- and part-time University employees, as well as wage payroll and paid interns.
- **Enterprise** – Enterprise refers to any resource that is installed, deployed, offered and/or managed centrally by the College of the Liberal Arts or Penn State University.
- **Extranet** – A computer network that allows controlled access from the outside, for specific business or educational purposes.
- **Jump Server -** a special-purpose computer on a network typically used to manage devices in a separate security zone. The most common example is managing a host in a DMZ from trusted networks or computers.
- **Network Data Loss Incident** - When a compromised computing resource has communicated with remote addresses on the Internet that are known or believed to be associated with illegal activity.
- **Notification** - The process of contacting those whose personal data may have been disclosed during a Data Loss Incident.
- **Personally Owned Equipment** - Equipment that was purchased with personal funds and is owned by the individual.
- **PII** – Personally Identifiable Information. Defined by the Pennsylvania Breach of Personal Information Notification Act as:
    - An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the name and data elements are not encrypted or redacted:
        - Social Security Number.
        - Driver's license number or a state identification card number issued in lieu of a driver's license.
        - Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.
        - Per Penn State practice, even if a security code, access code or password does not exist (but all other criteria match), it is still considered reportable PII.

- **Primary User** - The individual to whom the computing asset is assigned for routine or temporary use. If the asset is a shared resource then the Primary User is, at any given time, the active user.
- **Registered Owner** - The full-time faculty or staff member to whom the computing asset is officially allocated or entrusted. Students, part-time employees and non-employees may be a Primary User, but not a Registered Owner. For departmental assets such as staff workstations, labs or kiosks, The Department as an entity serves as the Registered Owner.
- **Remediation** – Removal of PII data from a computing resource.
- **SOS / Security Office/Privacy Office** - Security Operations and Services - The Penn State Security Office and the Penn State Privacy Office. The Security Operations and Services and The Penn State Security Office reference the same unit. The Penn State Privacy Office is a completely separate unit within the University.
- **Users** – Refers to all employees and/or any user that uses a University/College owned computing resource. This may include, but is not limited to, undergraduate students, graduate students, temporary workers, non-PSU faculty, non-PSU students, unpaid interns, consultants, contractors, vendors, and anyone who uses and/or connects to the CLA Network
- **Workstations or Computers** – refers to any computing resource that is owned by the College of the Liberal Arts. The computing device could refer to desktops, laptops, notebooks, netbooks, tablet, tablet PC, server, mobile devices, PCs, Macs, Apple, any distribution of Linux and/or Unix.

Information Security Roles and Responsibilities

Overview

College of the Liberal Arts information must be protected from unauthorized disclosure, loss, unauthorized modification, or any contingency that makes the information unavailable.

Responsibilities

ITLA Management Team

The ITLA Management Team is responsible for ensuring the integrity, confidentiality, and availability of all critical information assets, as well as setting policy, enforcing procedures, and implementing appropriate countermeasures. The IT Director is the principal contact for all security related incident responses.

Technical Staff and System Administrators

Technical staff and system administrator personnel are responsible for implementing technical information assurance procedures, as well as assuring that systems are appropriately configured to support this site security policy.

Employee and User Responsibilities

All employees and users are responsible for maintaining the College of the Liberal Arts' public image and using its resources in a productive manner.

Employees and users are responsible for information asset protection. While College IT and Network Security groups are responsible for providing physical and technical security, every employee and user

must understand the need for and participate in the protection of information assets, systems, and networks within Liberal Arts.

Employees and users are responsible for safeguarding both University proprietary information and information provided in confidence from other federal, state, local, and educational institutes. Employees and users must also respect the confidentiality of other employees' and users' electronic files and communications.

Employees and users are responsible for scanning their own data to ensure that any and all PII are remediated.

Management

College IT Managers are responsible for ensuring that all employees are aware of this site security policy. Managers must ensure that employees are able to identify, safeguard, and handle proprietary information and material. Managers and employees alike will be held accountable for safeguarding material and adhering to policies set forth by the College of the Liberal Arts.

Compliance with These Policies

All employees and users must comply with these policies. All computing devices connected, permanently or periodically, to the College of the Liberal Arts Network are subject to these policies. This includes, but is not limited to all wired connections, Liberal Arts-owned computers and laptops/notebooks assigned to Liberal Arts personnel or any other electronic device used to perform official duties as an agent of the University.

Employees and users who do not comply with this site security policy will be referred to Human Resources (HR) for disciplinary actions.

Continuous Assessment

The IT Management team must maintain an effort to continuously assess Liberal Arts' security posture. An effective and efficient security management program will address all aspects of the security lifecycle, which are assessment, protection, detection, and response. The fundamental first step – assessment - establishes the foundation for all protection, detection, and response policies and procedures. Due to its vital role, assessment will be performed continuously so the program will remain viable.

Identification and Authentication Policy

Unique ID

All computer systems must incorporate access controls that employ a unique identification code (User ID) for each user or automated process within Liberal Arts. All user IDs must be secured with a password.

The following standards must be used across all platforms:

- Each user of a system must have a unique User ID.
- Every identification code must be secured with authentication by password and/or SecureID tag/token and/or cryptographic keys.
- External access from outside of the Liberal Arts network requires 2 Factor Authentication

Passwords

Length, History, and Complexity

General User Population

Enforce password history	10 passwords remembered
Minimum password age	1 day
Minimum password length	12 characters

All passwords must meet the following complexity requirements:
Passwords may not contain your user name or any part of your full name.
Passwords must contain characters from at least three of the following four classes:

Description	*Example*
Upper case letters	A, B, C, ... Z
Lower case letters	a, b, c, ... z
Numerals	0, 1, 2, ... 9
Special characters	("!@,#$.%[/>\`~*

Examples of passwords that fit the requirements:
Low secure passwords: Password1 or 123Monkey
Very high secure passwords: T*6za2#B4/ or P/j>3$w@x)

Expiration and Change

Passwords must expire every 90 days. Reminders to change your password will begin 14 days prior to expiration. Only one password change by a user can take place within a 24 hour period.

Password Etiquette

Employees must protect all system user IDs and passwords, along with voicemail pin numbers, and e-mail account passwords at all times.
Individual passwords must NOT be printed.
Individual passwords must NOT be posted anywhere others can find it.
Individual passwords must NOT be shared with others.
Users must NEVER access any Liberal Arts computer system using another user's account or password.

Lost Passwords

In the event of a lost or forgotten password, the affected user must verbally request the account password be reset to the default password via the Liberal Arts help desk. Support staff must verify a user's identification prior to resetting any account. Questions will be asked to validate the identity of the user requesting the password reset.

User Responsibilities

Users in the College of the Liberal Arts are expected to comply with this policy. Employees and users who do not comply with this site security policy will be referred to Human Resources (HR) for disciplinary actions.

Other Authentication Mechanisms

When possible, restricted information should be protected by two-factor authentication.

All administrative access to servers where restricted information resides requires two-factor authentication. In addition, administrative access to all internal systems is restricted in that internal systems can only be accessed via the use of non-domain Jump Servers which also require two-factor authentication.

Policy Enforcement

Users of Liberal Arts systems are expected to comply with this policy, independent of the operating system's ability to ensure compliance.

Account Management Policy

Types of Accounts

User
User accounts are the primary and fundamental type of network access account for Liberal Arts systems. Every user must have a unique User ID.

Administrator
Administrator accounts provide super user and/or root access to servers and workstations. Administrator accounts are for system administrator job responsibilities and must ONLY be used for administrative purposes. Every system administrator must have a regular user account for non-administrative duties such as Internet access, word processing, and e-mail.

Group
Group accounts are established and authorized by special request only. Group roles or privileges are normally established to facilitate authorization and access control.

Guest
Guest accounts are to be disabled and are not permitted. A normal user account must be set up even if it is just for temporary access to systems.

Default
All default accounts must be renamed, disabled, or deleted on all workstations and servers.

Account Setup

New Standing Faculty User Account
New faculty user account requests must be submitted to the help desk by the Department Head or Administrative Assistant and include the user's complete name (first, middle initial, last name), employee designation (standing faculty, staff, FT1, FT2, Multiyear, or graduate student), Penn State Access Account information, and contact information, address, (e-mail and/or phone number), start date, and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, minimally one week prior to start date. The new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

New standing faculty user accounts will not be set up with expiration dates unless they are known to have a permanent end date. If the end date is known, then the user account will be set with an expiration date of the known end date.

New Staff User Account
New staff user account requests must be submitted to the help desk by the Department Head, Administrative Assistant, or new staff person's direct supervisor and include the user's complete name (first, middle initial, last name), employee designation (standing faculty, staff, FT1, FT2, Multiyear, or graduate student), Penn State Access Account information, and contact information, address, (e-mail and/or phone number), start date, and what network resources they will need access to, if known. The

request must be submitted as far in advance as possible, minimally one week prior to start date. The new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

New staff user accounts will not be set up with expiration dates unless they are known to have a permanent end date. If the end date is known, then the user account will be set with an expiration date of the known end date.

New FT1 or Multi-year User Account

New FT1 or Multi-year user account requests must be submitted to the help desk by the Department Head, Administrative Assistant, or new staff person's direct supervisor and include the user's complete name (first, middle initial, last name), employee designation (standing faculty, staff, FT1, FT2, Multiyear, or graduate student), Penn State Access Account information, and contact information, address, (e-mail and/or phone number), start date, and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, minimally one week prior to start date. The new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

New FT1 or Multi-year user accounts will not be set up with expiration dates unless they are known to have a permanent end date. If the end date is known, then the user account will be set with an expiration date of the known end date.

New FT2 User Account

New FT2 user account requests must be submitted to the help desk by the Department Head, Administrative Assistant and include the user's complete name (first, middle initial, last name), employee designation (standing faculty, staff, FT1, FT2, Multiyear, or graduate student), Penn State Access Account information, and contact information (e-mail or phone number), start date, and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, minimally one week prior to start date. The new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

The new FT2 user account will be created with an expiration date. The date of expiration will be the Monday following the date of Commencement of the assigned semester.. The Commencement dates can be found here… http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

If the end date is known and is later than the assigned semester, then use that date as the expiration date.

New Graduate Student User Account

New graduate student user account requests must be submitted to the help desk by the Department Head, Administrative Assistant, Graduate Director, or Graduate Assistant and include the user's complete name (first, middle initial, last name), employee designation (standing faculty, staff, FT1, FT2, Multiyear, or graduate student), Penn State Access Account information, and contact information (e-mail or phone number), start date, and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, minimally one week prior to start date. The

new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

The new graduate student user account will be created with an expiration date. The date of expiration will be the Monday following the date of Commencement of the assigned semester. The Commencement dates can be found here…
http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

New Undergraduate Student User Account

New undergraduate student user account requests must be submitted to the help desk by the faculty member, or staff member who the student will be working for and include the user's complete name (first, middle initial, last name), Penn State Access Account information, and contact information (e-mail or phone number), start date, end date (if other than end of current semester), and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, minimally one week prior to start date. The new user shall be provided with a username and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

The new undergraduate student user account will be created with an expiration date. The date of expiration will be the Monday following the date of Commencement of the assigned semester. The Commencement dates can be found here… http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

If the end date is known and is later than the assigned semester , then use that date as the expiration date.

New Non-Traditional User Account

All new non-traditional user account requests (non-Penn State faculty, non-Penn State student, visiting faculty, work study, wage payroll, interns, vendor, consultant, etc) must be submitted to the help desk by the faculty member, or staff member whom the "other" user account will be working for and include the user's complete name (first, middle initial, last name), Penn State Access Account information (if applicable), and contact information including other University/College name and department, address, (e-mail and/or phone number), start date, end date (if other than end of current semester), and what network resources they will need access to, if known. The request must be submitted as far in advance as possible, a minimum of one week prior to start date. The new user shall be provided with a user ID and an initial password that will be used to log into the domain the first time. The user account must be configured in a way that requires the user to change the password at first login.

The new non-traditional user account will be created with an expiration date. The date of expiration will be the Monday following the date of Commencement of the assigned semester. The Commencement dates can be found here… http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

If the end date is known and is later than the assigned semester, then use that date as the expiration date.

Re-enabling User Accounts or Resetting Password

For all user accounts that have expiration dates and the user is known to continue work after the expiration date, then the direct supervisor or principal faculty member that manages the project is required to submit a help desk request asking stating the person is continuing to work past their expiration date. This request should be submitted as soon as it is known the person will be continuing to work after expiration date to avoid delays in re-enabling the user account.

Before re-enabling an account or resetting a password, the IT Support person must obtain verification of the user's identity. Verification can be achieved through any of the following means: photo-ID; grad/faculty/staff whom you know vouching for the undergrad; grad/faculty/staff person via phone if you recognize the voice; knowing the person for in-person requests. If an account needs to be reset for a person whom you do not know and who does not present photo ID (i.e. if the person is from another University and/or cannot come on-campus to present photo ID), then identity confirmation from the associated Liberal Arts faculty/staff member must be established prior to re-enabling or resetting password.

A request to re-enable or reset a password for a user's account by anyone other than the user themselves is strictly prohibited.

Account Modification

Account changes/modifications must be requested in writing (help desk ticket) and approved by the employee's supervisor or manager prior to being implemented by the administrator.

Account Termination

Procedures must be in place to ensure that user identification codes (user IDs) are removed or disabled from all systems when users are terminated, transferred, or no longer require access.

Normal Termination Notification

Standing Faculty, FT1, FT2, Multi-year

All standing faculty, FT1, and Multi-year departures/terminations will be sent by the HR office to the IT Support staff in writing (help desk ticket) to provide the effective date of departure/termination.

After notification, IT staff will subsequently disable the user account on the date of departure/termination. Under normal circumstances, the IT staff is responsible for ensuring proper backup of desktop institutional business files upon employee departure.

Staff

Termination notices for all departing staff employees will be sent by the HR office to the IT Support staff in writing (help desk ticket) to provide the effective date of departure/termination.

After notification, IT staff will subsequently disable the user account on the date of departure/termination. Under normal circumstances, the IT staff is responsible for ensuring proper backup of desktop institutional business files upon the employee's departure.

Graduate Students

All graduate student departures/terminations will be reviewed by either the supervisor or by the department's graduate staff assistant at the beginning and end of each semester (Spring, Summer, and Fall); then notifications will be sent to the IT Staff in writing (help desk ticket) to provide the effective date of departure/termination if other than the normal four-year expiration date.

After notification, IT staff will subsequently disable the user account on the date of departure/termination. Under normal circumstances, the IT staff is responsible for ensuring proper backup of desktop institutional business files upon employee departure.

Undergraduate Students

The new undergraduate student user account will be created with an expiration date.The date of expiration will be the Monday following the date of Commencement of the assigned semester. The Commencement dates can be found
here… http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

After notification, IT staff will subsequently disable the user account on the date of departure/termination. Under normal circumstances, the IT staff is responsible for ensuring proper backup of desktop institutional business files upon the employee's departure.

Other

All non-traditional user accounts (non-Penn State faculty, non-Penn State student, visiting faculty, work study, wage payroll, interns, vendor, consultant, etc.) will be created with an expiration dateThe date of expiration will be the Monday following the date of Commencement of the assigned semester. The Commencement dates can be found
here… http://www.registrar.psu.edu/academic_calendar/calendar_index.cfm

After notification, IT staff will subsequently disable the user account on the date of departure/termination. Under normal circumstances, the IT staff is responsible for ensuring proper backup of desktop institutional business files upon the employee's departure.

Extending or Renewing Expired Accounts

If any user account that is set to expire and is to be extended or renewed the following session or semester (i.e. continues to work on the same project), the supervisor or employee's manager must submit in writing to the help desk a request asking that the account be renewed. This request must be submitted prior to the end of the semester or risk the account expiring causing delays in work.

Emergency Notifications

Notice of termination may be communicated verbally by HR to IT Managers when the termination of an account must be expedited. It is critical that access to system(s) be disabled immediately in emergency cases.

Accounts must not be deleted until the manager has an opportunity to review the desktop and server file storage directories. Final determination to delete disabled accounts resides with Liberal Arts IT Managers.

Account Lockout

A user's login account must be automatically locked after five unsuccessful login attempts. The user must then contact the help desk to revalidate and unlock their account. Locked accounts will be reset automatically after 35 minutes.

Authorizations

Account Privilege Permissions

By default, new accounts must be created with the fewest privileges available. Each IT Support staff member is responsible for determining for their unit the appropriate access requirements of every employee based upon their job responsibilities

Once a user has authenticated to the Liberal Arts domain, they must have access only to those network resources deemed appropriate to their job function.

Administrator, super user and other root access privileges must only be granted to administrators with the need for such access within their job responsibilities, and must be granted the least privilege required to perform their duties.

File Privileges

Shared file folders must be established with a least-privilege approach. By default, files within a shared folder are accessible only to the owner(s). The file owner(s) is responsible for explicitly determining file privileges for wider distribution by requesting in writing via a help desk ticket (1) additional users and (2) the explicit privileges to grant (modify or read-only) for those users.

Local Administrative Rights, Root Access, Super-User Privileges

Users are not granted administrative, root, or super-user rights to their workstations or laptops. Specifically, users are prohibited from:

- Installing unlicensed software
- Creating additional user accounts
- Editing user accounts
- Editing/Changing Security Permissions or Settings
- Allowing other family members, friends, or associates to use University/College-owned computing devices
- Installing network monitoring tools/utilities
- Use of Freeware that is not business related
- Installing alternative operating systems (Linux, Unix, Windows, Mac) on top of primary operating system without explicit approval from Liberal Arts IT Management Team
- Un-installing pre-configured software (i.e. anti-virus)

Users may request an exception to establish administrative rights through a separate local administrative account that will be used for the sole purpose of the justified reason given (not as a regular use account), or the regular domain user account will be added to a specialized group that will be managed through a centralized privilege rights application. These rights will be reviewed annually to

determine ongoing support for such rights. These exceptions will be granted by the Liberal Arts IT Director and may change without notification.

Regardless of the level of administrative access to any workstation, users are not permitted to make any changes to the network configuration established by Liberal Arts IT.

Acceptable Use Policy

General Use and Ownership

Computers, mobile devices, network connectivity, wireless, Internet and Intranet access, voicemail, electronic mail, telephony, and other communications systems are all part of the CLA Network and are provided by The Pennsylvania State University and the College of the Liberal Arts. These resources are provided to assist employees and students in obtaining work-related data and technology and effectively communicating work-related information. The following policies have been established to help ensure responsible, secure, and productive Internet, Intranet, network connectivity, and computer usage.

Expectation of Privacy

Recognizing the College's responsibility to protect employees' personal privacy and dignity, Liberal Arts must exercise great care and judgment in the collection, maintenance, use, and release of employee personal information. However, when using organizational computer assets, employees should not expect any extraordinary privacy regarding their actions. All usage of the computer systems must be in accordance with University policy and usage expectations.

Liberal Arts-owned and provided personal (secondary) computers are areas where the University's business information and employees' personal information are likely to become commingled. For the majority of employees, and for most of the time, there is no problem with such commingling. However, for security reasons, it may be necessary for management to scan an employee's computer for personal identifiable information other than the employee's, and it is important for employees to understand that the University Security Office and the College Management Team have the legal right to do so.

Personally Identifiable Information (PII)

The University provides PII scanning software free of charge for all university-owned equipment. Installation and active use of this software is required for all devices connected to the CLA Network. Additional details are available in the PII Scanning Policy section of this manual.

Monitoring Usage

Computers are subject to electronic monitoring to determine usage patterns such as logon date and times, duration of active use, and number of unique users. In order to manage the traffic within the College's internal network and to protect networks and systems from external threats, all network segments and network workstations are subject to monitoring and auditing. Questions regarding this policy and the College's information management practices may be directed to the IT Manager or to the Director of Administrative Services for explanation and guidance.

Reasons Why Liberal Arts Would Scan Computer and Files Server Data

Reason	Scans Performed	Timeline
Search for Security Vulnerabilities	antivirus and spyware	weekly
Security Risk Assessment	port scan and software vulnerability	quarterly
Suspected Compromise/Suspicious Threat, Network Anomaly	text string based scan	as needed
Personally Identifiable Information	text string based scan	At least once every 30 days

Under no circumstance will Liberal Arts management or staff scan employee computers unless for reasons given above and/or legal matters.

Personal Usage

Employees, Primary Owners, or Users may not install or download any non-business; non-academic related software, whether from the Internet or other sources. Examples of such software are personal tax software, games, peer-to-peer file sharing/networking software. Additionally, the installation of software that is for personal preference over that which the college already supports and has installed for use is strictly prohibited. An example of such software would be alternative web browsers like Opera or SeaMonkey. Only Liberal Arts IT staff members are authorized to install software on Liberal Arts computer systems. Employees, Primary Owners, or Users requiring assistance should contact the IT Help Desk or submit a help desk ticket.

Allowing family members, friends, or associates to use your assigned computing device that are not directly employed by the College of the Liberal Arts is strictly prohibited.

Please see University policy AD20 – Computer and Network Security, and AD23 – Use of Institutional Data, and AD53 – Privacy Statement for full definitions regarding appropriate use of University-owned computing equipment.

Trap Doors

Programmers and other technically-oriented staff or faculty are prohibited from installing trap doors or other methods that circumvent the authorized access control mechanisms found in the operating systems and/or access control packages.

Encryption

Encryption must be used when transferring sensitive or confidential university data over an unsecured network link. Every general-purpose encryption algorithm used to protect Liberal Arts production information and information systems must meet or exceed the AES-128 algorithm standard.

Prohibited System Usage

Data that is composed, transmitted, stored, or accessed through our computer systems over the Internet or Intranet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or other person ("offending data"). Employees who receive offending data must notify the sender that the sender is not to transmit such data again, and that receipt of such data in the future will result in notification of the Penn State security office. Examples of offending data may include, but are not limited to, racial slurs, sexual comments or images, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law. Additionally, harassment by communication is prohibited. Under no conditions should sites that deal with or promote sexual conduct or violence be accessed from or through any College computer.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet or Intranet is expressly prohibited. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights. If an employee has any reason to believe that material received would violate this policy, it should be deleted.

Personal and otherwise sensitive information including, but not limited to, Social Security numbers, credit card numbers, driver's license numbers, and bank account numbers are also prohibited on any College computer, file server, or any network device connected to the College network.

The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's time and unauthorized use of resources for personal gain
- Stealing, using, or disclosing someone else's code or password without authorization
- Copying, pirating, or downloading software and electronic files without permission
- Sending or posting confidential material or proprietary information outside of the organization
- Violating copyright law
- Failing to observe licensing agreements
- Participating in the viewing or exchange of pornography or obscene materials
- Sending or posting messages that defame or slander other individuals
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation
- Sending or posting chain letters, solicitations, or advertisements of an inappropriate nature

Content related to performing the employee's job responsibilities is not offending data under this policy, and therefore, is not prohibited to the extent it is needed to perform legitimate job responsibilities, such as research.

Except in cases when Liberal Arts management has granted explicit authorization, employees are prohibited from engaging in or attempting to engage in:

- Monitoring or intercepting the files or electronic communications of other employees or third parties
- Breaching, testing, or monitoring computer or network security measures.

Employees must not use networks and systems in a manner that is likely to cause network congestion or significantly hamper the ability of other employees to access the system.

Misuse

Misuse of the institution's electronic communications systems is serious misconduct and may result in discipline up to and including termination. If you have any questions regarding computer usage, please contact a human resources representative. If you have been subjected to inappropriate material through your computer or someone else's computer, please contact your supervisor or an HR representative.

Alter or Move Hardware

Tampering with, altering, or changing any hardware on a Liberal Arts-owned computing resource is strictly prohibited without either the knowledge of or the express written consent of the local IT Support staff.

Moving or relocating Liberal Arts-owned computing resource from its permanently assigned office is strictly prohibited without either the knowledge of or the express written consent of the local IT Support staff. Mobile devices intended to be mobile are permitted to be moved.

Accountability

Users are accountable for their actions when using the College network. However, user accountability is predicated upon providing appropriate protections to user IDs, passwords, and pin codes. Employees are responsible for work performed under their passwords and/or access codes; therefore, employees must maintain the confidentiality of their system passwords. Anyone obtaining electronic access to another institute, company, or individual's materials must respect all copyrights and cannot copy, retrieve, modify, or forward copyrighted materials, except as permitted by copyright owner.

Administrator Account Password Escrow

All administrative and root passwords must be stored in an encrypted secure password repository.

Administration Policy

Account administration procedures must be consistent for all Liberal Arts systems, and must comply with this site security policy and the Liberal Arts Business Processes and Active Directory Administrative Model - 1.3 (this document is internal to IT Staff as a Standard Operating Procedure manual).

Data Protection Policy

Laptop/Notebook/Netbook Computers

Reasonable care must be taken to ensure that all proprietary data processed on laptop/notebook/netbook computers are not vulnerable to exploitation if the laptop is lost or stolen. Thus, all laptop/notebook/netbook computers owned by Liberal Arts must be whole disk encrypted by software approved by the IT Management Team of the College of the Liberal Arts.

Internal Restricted or Sensitive Information

Although measures are in place to protect critical Liberal Arts information from disclosure to outside parties, certain types of data are extremely sensitive and restricted in its use, and must be tightly protected within Liberal Arts controlled areas. These information categories include executive correspondence, passwords, router configurations, firewall rule sets, system security logs, and personally identifiable information. All information in these categories must be encrypted in transmission and remain encrypted in storage and or at rest.

Encryption

Encryption must be used when transferring sensitive or confidential university data over an unsecured network link. Every general-purpose encryption algorithm used to protect Liberal Arts production information and information systems must meet or exceed the AES-128 algorithm standard.

Personally Identifiable Information (PII) Policy

Introduction

This section sets forth the policy for the handling of Personally Identifiable Information (PII) in the College of the Liberal Arts. Requirements and definitions are taken or derived from the Pennsylvania Breach of Personal Information Notification Act, the Penn State PII scanning initiative, and Penn State Policy AD-19. If there is contradiction between this policy and the aforementioned resources, Pennsylvania legislation and Penn State policies are to be considered authoritative. All computing devices connected, permanently or periodically, to the College of the Liberal Arts Network are subject to this policy. This includes, but is not limited to all wired connections, Liberal Arts-owned computers and laptops/notebooks assigned to Liberal Arts personnel or any other electronic device used to perform official duties as an agent of the University. PII data may not be stored on any electronic asset in the College of the Liberal Arts unless a formal authorization has been granted by the Dean and the Penn State Privacy Office.

Scanning

Periodic PII scanning (currently set to every 30 days) and subsequent remediation are required for all workstations, laptop/notebook computers, servers and network storage devices on the College of the Liberal Arts Network.

All electronic devices must be scanned by SOS-approved PII scanning software (currently Identity Finder), either via scans setup to run automatically every 30 days, or manually by the primary user and/ or users every 30 days or via network scans by one of the IT staff appointed by the IT Management Team.

Identity Finder is licensed for all University-owned equipment, but not personal devices. Any device that is not compatible with this approach is subject to a “best-effort” using alternate scanning methods (such as Spider) or manual review of data.

Scans performed by the college will only search for text strings consisting of Social Security number, credit card number, driver’s license and bank account number formats. These scans are done by searching the computer for specific text strings via a pre-scripted routine. Employees are not permitted to keep personally identifiable information of themselves or of their family members on their Liberal Arts-owned computing resources, including , but not limited to, desktop computers, laptop/notebook/netbook/tablet computers, external hard drives or thumb drives, or Liberal Arts file servers. The University and Liberal Arts will not be liable for your own personally identifiable information becoming compromised if you choose to keep this information on your University/College owned computing resource or on Liberal Arts servers.

Devices must be scanned at least once every 30 days. Any device that has been scanned by Identity Finder and reported free and clean of PII within a 30-day history are not required to undergo further scanning in the event of a compromise.

Remediation

Upon completion of a PII scan, subsequent remediation is required to remove the PII from the computing resource and earmark any false positives.

Subsequent remediation in terms of Identity Finder means immediate remediation. Identity Finder is set up in guest mode and scan results cannot be saved, therefore, remediation is required immediately upon scan completion.

Network Access

Network connectivity may not be granted unless Departmental IT Staff have verified the installation of PII scanning software, antivirus software installed with automatic virus definition updates enabled, and both the Primary User and Registered Owner have signed the PII User Agreement (PUA). The following requirements are needed on the PUA:

- Signature(s) of the Registered Owner and Primary User (when applicable) indicating review and acknowledgement of understanding of this policy is/are present.
- Penn State ID, Date and Department

The PUA is bound to an individual, and must be kept on file as long as any asset officially associated with that individual as a Registered Owner or Primary User remains on the network and/or is actively used for University business. Operation of a computing asset on the College of the Liberal Arts network without PII scanning software (or equivalent as necessary) properly installed and actively used is a violation of the Acceptable Use Policy.

Roles and Responsibilities

Primary User

The Primary User of a workstation is responsible for remediation of the resource to the extent that their system rights permit. If the asset is a shared resource then the Primary User is, at any given time, the active user. Sufficient authentication and logging must be in place so that system access can be correlated to a particular user at a particular time.

Registered Owner

The Registered Owner is responsible for oversight, ensuring that the systems in their care are properly scanned and remediated as necessary. Any financial cost incurred as a result of a compromise and/or notification is the responsibility of the Registered Owner. The Registered Owner must maintain an accurate accounting of their Primary Users should assets be re-allocated after PII User Agreement was signed.

Consequences

Individual employees (registered owners) may or will be held responsible if they were found to be willfully negligent or irresponsible in complying with the processes described herein. This discipline may include reprimand, denial of access to computer resources, and/or termination of employment.

IT Staff

IT Staff are responsible for:

- Scanning network storage, servers, and administratively-restricted areas of user computer or laptop/notebook/netbook.
- Collecting and storing PUA's prior to establishing a network connection.
- Reviewing console reports at least once a quarter to verify that users are actively remediating their scan results.

The College of the Liberal Arts

The College will provide access to necessary software, create documentation (or refer to existing documentation), develop training materials, and serve as an additional level of user support for PII scanning and remediation efforts.

Exceptions

If a unit within Liberal Arts requires the use of PII as part of their business function or needs to save/store PII in order to complete tasks as required by the unit, the Dean, IT Management, and the Financial Officer will evaluate this requirement and request a formal exception through the University SOS, Risk and Privacy Offices. If an exception is granted, additional security measures are required by the unit. These measures are defined in the section titled "Personally Identifiable Information Exception Policy".

Personally Identifiable Information (PII) Exception Policy

Introduction

This section sets forth the policy for handling exceptions that would allow the use of Personally Identifiable Information (PII) in the College of the Liberal Arts. All computing devices connected, permanently or periodically, to the College of the Liberal Arts network are subject to this policy. This includes, but is not limited to all wired connections, wireless connections, Liberal Arts-owned computers and laptops/notebooks assigned to Liberal Arts personnel or any other electronic device used to perform official duties as an agent of the University. PII data may not be stored on any electronic asset in the College of the Liberal Arts unless a formal authorization has been granted by the Dean and the Penn State Privacy Office.

Requests for Exceptions

Prior to Liberal Arts making a formal exception request, the unit Head, Director and/or Supervisor is required to submit a help desk ticket to request a meeting with Liberal Arts IT Management team to discuss why an exception is needed.

Upon agreeing that an exception request is warranted, IT Management team will submit a formal exception request to the Dean and the Penn State Privacy Office.

Furthermore, a questionnaire will need to be filled out that is hosted by the Privacy Office. The questionnaire will help evaluate the risks and identify areas of concern that require more scrutiny.

Additional Computer Security Requirements

If an exception is granted, additional computer security is implemented and followed on the computers, servers, and networks within the Unit granted the exception.

The additional computer security will come from a joint effort of the University Privacy Office and the University Security Operations and Services Units. These additional security practices will be unique to each Unit that is granted an exception. The College of the Liberal Arts IT Management team, as well as, IT Support and Systems Administrators will help implement the additional security measures needed to comply with University guidelines when an exception is granted. These additional security practices will be held, maintained, and updated by the College IT Management team and the joint offices of the University Privacy Office and the University Security Operations and Services Units.

Additional Unit Specific Policies, Procedures, and Protocol Requirements

In addition to the extra layer of computer security implemented, the Unit will establish its own policies, procedures, and protocols specific to how it handles and secures PII within the Unit.

These Unit specific policies, procedures, and protocols will be reviewed by the Director of the Unit, as well as, the College's IT Management team. The compliance of these policies, procedures, and protocols within the Unit are the responsibility of the Unit Head or Director.

Additional Unit Specific Change Control and Configuration Management Requirements

In addition to the extra layer of computer security implemented, the Unit will establish its own change control and configuration management. Change control will entail documentation for all changes to procedures and or configurations to servers, computers, network components, etc. The change control and configuration management for the policy and procedures defined will be handled by the Unit itself. The change control and configuration management for all servers, computers, and network components will be handled by the Liberal Arts IT management team and their staff.

These Unit specific change controls and configuration management will be reviewed by the Director of the Unit, as well as, the College's IT Management team. The compliance of these change controls and configuration management requirements within the Unit are the responsibility of the Unit Head or Director in association with the Liberal Arts IT Management team if the change control and/or configuration management deals with information technology components.

Annual Exception Review/Renewal

In additions to the policies, Annual reviews will be conducted by IT Management to re-evaluate the need for an exception, as well as, audit the Unit for compliance of the new policies, procedures, and protocols. Additionally, the annual review will include updates, questionnaires, and any technology changes to the environment that may be needed to maintain compliance.

Annual reviews will be conducted by the University Privacy Office. The review process will be carried out with the help of Liberal Arts IT Management team with the Unit given the exception. Additionally, annual reviews will be done by IT Management to re-evaluate the need for an exception, as well as, audit the Unit for compliance of the new computer security practices, policies, procedures, and protocols. The annual review may include updates, questionnaires, and any technology changes to the environment that may be needed to maintain compliance.

Non-Compliance

If it is discovered that the computer security practices and or the Unit specific policies, procedures, and protocols are not being followed, or otherwise found to be willfully negligent or irresponsible in complying with the processes described within the customized practices, the Unit may lose its personally identifiable information exception status. Additionally, individual employees (registered owners) may or will be held responsible if they were found to be willfully negligent or irresponsible in complying with the processes described in said documents. This discipline may include reprimand, denial of access to computer resources, and/or termination of employment.

IT Incident Response Policy

Introduction

The purpose of this policy is to outline a standard set of actions and roles in the event of an IT security incident in the College of the Liberal Arts. The procedures and statements contained in this document are intended to supplement, not supersede, policy provided by the Privacy Office, Security Operations, and the University.

Compromise

In the event of a suspected compromise, the affected computer(s) must be removed from the network immediately, brought to the security office by the Technical Contact, and scanned for PII using deep-search software provided by the Security Office (currently Identity Finder). If any removable media was plugged into the computer at the time of compromise, the removable media is required to remain in place because it needs to be scanned for PII.

The only exception is when the compromised resource has been part of routine scans (using SOS-approved software) and reported free and clean of PII 30 days or less before the compromise occurred. In this latter case, the compromised resource may be rebuilt upon confirmation with SOS.

Technical Contact

Assignment of a Technical Contact is required for all security incidents and may be any full-time IT Support Staff selected by the IT Management team. This may be a standing selection for all occurrences. The primary user of a compromised resource may serve as a Technical Contact only in a shared role with a second individual.

The Technical Contact is responsible for communication and coordination with the Security Office, and for overseeing the scanning procedure. The scanning process may be delegated, but the responsibility for correct execution and delivery of the scan results remains with the Technical Contact.

Administrative Contact

The Administrative Contact can be a person on the IT Management team of the College. This may be a standing selection for all occurrences.

The Administrative Contact is responsible for all actions required as a result of the compromise such as the removal of PII data as directed by the Security Office and/or the Technical Contact, review of relevant security policies with unit faculty & staff, and processing of paperwork.

These actions may be delegated, but the responsibility for accuracy and completion remains with the Administrative Contact.

Data Loss

If the scanning procedure uncovers PII on the compromised machine, there is the potential for a Data Loss Incident. The Security Office will review log data from the network border and inform the Technical Contact whether or not further analysis is required and whether or not the incident will be passed on to the Privacy Office for determination of notification requirements.

Notification

Pursuant to the Pennsylvania Breach of Personal Information Notification Act (Senate Bill #712: http://www2.legis.state.pa.us/WU01/LI/BI/BT/2005/0/ SB0712P1410.pdf), all computer security incidents involving the potential for loss of PII data require notification be made to the individuals whose information may have been compromised. The process of notification must be given priority and completed as rapidly as possible.

Project Manager (PII only)

Assignment of a Project Manager is necessary only when notification is required. This role will be appointed by the Dean to oversee the notification process. The Project Manager must be a member of the IT Management team, and may or may not be the same person who served as the Administrative Contact for the initial incident. The individual(s) directly responsible for a workstation or server involved in the incident are not eligible to be the Project Manager.

The Project Manager is responsible for the successful completion of the notification process, and for ensuring compliance with privacy requirements by all College of the Liberal Arts personnel involved with the incident. Required actions may be delegated, but the responsibility for their accuracy and completion remains with the Project Manager.

IT Liaison (PII only)

Assignment of an IT Liaison is necessary only when notification is required. The Project Manager will coordinate with the unit IT Staff to appoint an IT Liaison for the duration of the notification process; this may or may not be the same person designated as the Technical Contact for the security incident. The IT Liaison is the primary point of contact for all technological questions and actions, including creating secure network shares as a workspace for the Project Manager and Support Staff, formatting and rebuilding a compromised computer, providing encryption mechanisms, and serving as a technical advisor to the Project Manager. At the discretion of the Dean and the Project Manager, the IT Liaison and other IT Staff may or may not be involved in parsing data.

Support Staff

The Project Manager may delegate required actions to any number of support staff provided the selection of such staff and the estimated time requirement is first coordinated with their supervisor. These actions may include, but are not limited to, printing and mailing letters and parsing PII data. The manning of a call center may not be delegated to support staff; only the Project Manager or a Penn State-approved, contracted, external company may take calls regarding a notification.

Actions

The procedure for notification is outlined in the Sensitive Data Exposure Incident Kit provided by the Privacy Office. Modification to the procedure is not permitted, and strict adherence is expected. However, customization of the notification letter and the scripted "FAQ" responses is permitted and falls under the responsibility of the Project Manager.

Privacy

The privacy of involved parties must be respected at all times. This includes those who have had their information compromised as well as the person(s) on whose computer the information was located. Access to PII data during incident response should be restricted as much as possible without impeding the required processes. Information regarding the general location and scope of the incident may be shared when security has closed the case and, when applicable, after notification letters have been sent out. The identity of the person(s) from whose computer the information was compromised may not be shared except as necessary to complete the investigation and/or notification process.

Reporting

The Technical Contact is required to record and provide the following information to the IT Management team for all IT security incidents:

- Date of Incident
- IP Address of Compromised Resource
- MAC Address of Compromised Resource
- Name of Technical Contact
- Name of Administrative Contact
- Whether or not Notification was required
- Name of Project Manager (when applicable)
- Name of IT Liaison (when applicable)
- Date of Mailing for Notification Letters (when applicable)
- Brief Summary
- Date of Incident Resolution

This data must be submitted to the IT Director within one week of incident resolution and must be retained for 6 years.

Summary

The timely execution of the notification process is an essential component of regaining the trust of the affected individuals, and maintaining the integrity of our reputation. Questions, suggestions, or requests for clarification may be sent to the IT Director of the College of the Liberal Arts.

Session Controls Policy

Login Banner

The College of the Liberal Arts computers and network systems are provided to support appropriate business and organizational purposes. Best practices for protecting information technology resources dictate that access attempts be preceded with a warning banner prior to system entry. The following warning banner must be displayed when users connect to the internal computer networks:

> "This is a Penn State Liberal Arts computer system. This computer system, including related equipment and network (specifically including Internet access), are provided for authorized use as described in Penn State Policies AD20, AD23, and ADG02 and in Liberal Arts Security Polices. Liberal Arts computer systems may be monitored for lawful purposes as stated in Penn State Policy AD53 to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored to the extent specified by Penn State Security Policy. Use of this computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to administrative action or criminal prosecution as state in the Penn State Policies and Liberal Arts Security Policies. Use of this system constitutes consent to monitoring for these purposes."

Session Management

Unattended Workstations

All College workstation users must lock their screens – with password protection – before leaving them unattended.

Automatic Time Outs

Computer policy will lock the screen automatically after 15 minutes of inactivity on staff, graduate or lab computers and 60 minutes of inactivity on faculty office computers. Re-establishment of the session must take place only after the user has provided the proper password. Users are prohibited from circumventing the automatic timeout feature on College workstations.

End of Day

At the end of the day or working session, users must terminate all external (non-desktop) applications, and log off from their workstations.

Remote Access Time Outs

Remote access sessions from the Liberal Arts Remote Services Portal will time out after 30 minutes of inactivity.

Previous User ID

Workstations must not display the user ID of the previous user on the initial or subsequent login screen.

Clock Synchronization across Platforms

All multi-user computers connected to Liberal Arts internal network must always have the current time accurately reflected in their internal clocks.

Session Audit

Maximum Login Attempts

The number of consecutive attempts to enter an incorrect password is limited to five. After five unsuccessful attempts to enter a password, the account must be either: (a) suspended until reset by a system administrator, or (b) temporarily disabled for no less than 35 minutes.

Network Connectivity Policy

University Owned Equipment

Only University-owned equipment is permitted to connect via a hard wire connection to the Liberal Arts network. University-owned equipment includes, but is not limited to, equipment purchased with general department funds, grants (federal, state, foundation, company), startup funds, research account funds, or any funds originating from Penn State. University-owned equipment also includes any equipment purchased from another institution/entity via a grant, but which has since been transferred to Penn State.

Personally Owned Equipment

Personally owned equipment is prohibited from connecting via a hard wire connection to the Liberal Arts network. Personally owned equipment is equipment that was purchased with personal funds and is owned by the individual.

Switches, Hubs, Routers, Wireless Access Points

Switches, hubs, routers, and wireless access points are not permitted to be used/installed in any Liberal Arts-owned/leased office for the purposes of creating additional data jack ports or any other reason by individuals other than personnel approved by IT Management team. If additional physical data jack ports are needed, please contact the College Help Desk.

External Network Connectivity Policy

Authorization Procedures for Remote Access/Connections

Remote Access to College File Servers

Faculty and graduate students are granted remote access via the Liberal Arts Remote Services Portal. The Liberal Arts Remote Services Portal requires two-factor authentication. Faculty and graduate students are given access to their home directories and other departmental directories for which they have privileged access. This access is granted upon request.

Staff will not be given remote access to College file servers via the Remote Services Portal unless approved by the IT Management team.

For assistance and setup instructions, please contact the College Help Desk.

Remote Access to Office Computer

Remote access to an employee's office computer is granted if the following criteria are met:

- The individual is a staff (exempt) or full-time faculty member of the College of the Liberal Arts.
  - Exceptions are made for non-exempt staff and wage payroll personnel, however, requests for exceptions must be submitted via http://techsupport.la.psu.edu/forms/portal-access.
- The individual is connecting to a Liberal Arts-owned computer that is connected via a wired connection and is located within a Liberal Arts-occupied and managed building.
- The individual is the only person who uses the assigned on-campus computer (the computer cannot be shared).

Graduate students are given remote access to a computer only if a faculty member requires and requests such access and the graduate student is the only user of the assigned on-campus computer (the computer cannot be shared).

For assistance and setup instructions, please contact the College Help Desk.

Prohibitions

Unauthorized Services and Applications

Employees are prohibited from installing any services or applications on their local desktops without prior authorization.

Network Firewalls

The internal network is segmented into multiple VLANs designed to group similar devices such as faculty workstations, groups of servers, or particular services such as network file storage that contain sensitive data. All internal network traffic between VLANs is passed through the firewall, limiting connectivity.

Inbound and outbound traffic is also controlled with the firewall. Inbound traffic is restricted to a select group of services which are required for normal business functions. For internal enterprise servers and services, outbound traffic is restricted based on the required device functionality. Outbound traffic from workstations is restricted based on URL categorization from a 3rd party security vendor.

Mobile Devices Policy

Institutional Data - Regardless of Personally Owned or University Owned

Per University Policy FN21 "All institutional data must be protected from unauthorized disclosure and must be protected with the same granularity of security control provided by the originating host system. This includes institutional data on mobile devices, including personal devices which may be used for business purposes. Certain private data, such as social security numbers, may not be retained on local or mobile devices unless an exception has been granted by the University Privacy Officer. "

To clarify this policy further, all institutional data (any data generated by Penn State, copied from Penn State, or otherwise owned by Penn State) must be protected by the person who has possession of the data on any device (including, but not limited to personally owned devices at home and/or mobile devices (smartphones, tablets, laptops, MacBook's, etc.). Additionally, this data must be protected from unauthorized disclosure meaning that if you have institutional data on a personal computing device, then that system must be password protected to prevent unauthorized disclosure of said data.

University/College Owned

All mobile devices owned by the University/Liberal Arts must adhere to the following security controls to comply with the general University Policy FN21 explained above:

Windows Laptop or Apple MacBook on Liberal Arts Domain

These devices have the following controls to safeguard the data housed on the hard drive of the device:

1. The Liberal Arts domain security policies are active on these devices regardless of whether they are wired, wireless, or on Liberal Arts owned networks or not.
2. Password Protected
    a. Same password policy as laid out in this document under Identification and Authentication Policy.
3. Enforce Locking of the Screen After Non-Activity
    a. Same automatic time outs policy as laid out in this document under Session Controls Policy.
4. Encrypt the Hard Drive
    a. Same hard drive encryption policy as laid out in this document under Data Protection Policy.

Windows Laptop or Apple MacBook not on Liberal Arts Domain

These devices have the following controls to safeguard the data housed on the hard drive of the device:

1. Password Protected
    a. Same password policy as laid out in this document under Identification and Authentication Policy.
2. Enforce Locking of the Screen After Non-Activity
    a. Same automatic time outs policy as laid out in this document under Session Controls Policy.

3. Encrypt the Hard Drive
    a. Same hard drive encryption policy as laid out in this document under Data Protection Policy.

Tablets (iPad, Microsoft Surface or equivalent)

Liberal Arts has a separate policy (outside the scope of these security specific policies) on tablet computing that relates to the purchase, support, and management of tablets, which can be found here… https://intranet.la.psu.edu/ITLA/TabletComputingPolicy.pdf. There are a few security related policy statements in this policy; however, the following define specific controls.

These devices are managed by device management software (Casper or SCCM) to enforce security policies and controls that will safeguard the data housed on the device. These controls are implemented regardless of what network the device is connected to.

1. Password Protected
    a. Password policy is enforced
    b. Password length is 5 characters
    c. Password type is simple characters, so they could use numbers only.
2. Enforce locking of the screen after non-activity
    a. Inactivity time out is 1 hour before device screen will lock and force.
3. Enforce Encryption of the Hard Drive/Memory/Flash on the Device
    a. All data types and file types are encrypted on the device.
4. Remote Wipe the Device
    a. If a device is lost or stolen, we have the ability to remote wipe the device, thus resetting it back to factory setting deleting all data and apps that were on the device.
5. Quarantine When Out of Compliance
    a. When a device is out of compliance, meaning that if someone disables data protection, when someone disables MobileIron, when a compromised OS is detected, the device is put into Quarantine making it un-usable.

Acceptable Use

All mobile computing devices owned by Penn State/Liberal Arts must follow the acceptable use policies as laid out in this document under Acceptable Use Policy.

Personally Owned

Although Penn State cannot dictate or otherwise control or manage personally owned mobile devices, the owner is still responsible for implementing security controls that properly safeguard Penn State institutional data as outlined in University Policy FN21.

Auditing Policy

Systems for Auditing

All file servers and application systems that handle administrative information will log all additions, modifications, and deletions.

All Active Directory additions, modifications, and deletions will be logged.

All firewall additions, modifications, and deletions will be logged.

Parties Responsible for Audit and Audit Review

All system, application, and network administrators will regularly audit security-relevant log files generated by systems under administrative control. The IT Management Team specifies the audit method and frequency.

Audit Review Schedule

Audits will be reviewed on a daily, weekly, or on an as-needed basis to be determined by the type of data being collected by the auditing source.

Audit Reporting

The results of all system and application audits must be reported to the IT Management Team upon completion of the audit.

Audit Logs

Retention Period

Computerized logs containing security relevant events must be retained for at least (3) months and retained in accordance with University policy AD35.

Safeguards

During the retention period, audit logs must be secured such that they cannot be modified, and such that only authorized persons can read them.

Record Content - Security Relevant Events

Computer systems handling administrative information must securely log all significant, security relevant events. Examples of security relevant events include, but are not limited to, failed login attempts, administrative logon/logoff, network connections, restricted application accesses, restricted file accesses, firewall configurations, and intranet root logon attempts.

Logs of computer security relevant events must provide sufficient data to support comprehensive audits of the effectiveness of, and compliance with security measures.

All privileged commands issued by computer system operators must be traceable to specific individuals via the use of comprehensive logs.

All computer systems running production application systems must include logs which record, at a minimum: (1) user session activity, including user-IDs, log-in date/time, and log-out date/time, (2) changes to critical application system files, (3) additions and changes to the privileges of users, and (4) system start-ups and shut-downs.

Security Incidents

All security incidents must be reported immediately to the IT Management Team and then to the University's Security Office.

Virus Scanning Policy

College Workstations

The University provides antivirus software free of charge to anyone with a PSU ID. All computers owned by the College of the Liberal Arts must employ virus detection software. This software will be deployed centrally and may not be removed for any reason. Additionally, any system connecting to the CLA Network must also employ virus detection software. Liberal Arts reserves the right to scan your system to ensure you have antivirus software and that the virus definitions are up-to-date before you connect to the CLA network.

Signature Updates

Virus control software must be configured to seek a signature update from the vendor daily.

Scan Frequency

The anti-virus software must be running as a background process at all times. Additionally, the virus detection software must perform a full system scan on a weekly basis.

Scan Disable

Users are prohibited from disabling the virus scanning application on College computers.

Servers

All servers must employ virus detection software.

Signature Updates

Virus control software must be configured to seek a signature update from the vendor daily.

Scan Frequency

The anti-virus software must be running as a background process at all times. Additionally, the virus detection software must perform a full system scan on a weekly basis.

Laptops/Notebooks/Netbooks/Tablets

All laptop and portable computers must employ virus detection software.

Signature Updates

The software must be configured to seek a signature update from the vendor daily and, if disconnected from the network, will check as soon as reconnected. Additionally, users must not modify or disable the virus signature update schedule for the virus scanning application.

Scan Frequency

The anti-virus software must be running as a background process at all times. Additionally, the virus detection software must perform a full system scan on a weekly basis.

Scan Disable

Users are prohibited from disabling the virus scanning application on College laptops.

Anti-Virus on External Media

All external media must be subjected to a virus scanning procedure before any information contained on the media may be transferred to the College network.

All e-mail attachments must be subjected to a virus scanning procedure prior to being delivered to the e-mail recipient.

Virus Notification Process

Employees are required to notify their IT support staff immediately upon receipt of a suspected computer virus.

Change Management Policy

Configuration Control

All Liberal Arts servers, software, and networking systems used for production processing are considered critical systems. Accordingly, they must employ a formal change control procedure authored by the IT Management team, which is used to ensure that only authorized changes are made. Specifically, changes to the following systems will be determined and documented separately by the IT Staff responsible for those changes and approved by the Management team.

- College-wide software
- College-wide servers
- College-wide Web-site software
- College network security hardware
- College network security configurations

Desktop Workstation Configuration Changes

Desktop configuration changes are managed and deployed centrally. This includes, but is not limited to, operating systems, applications, firewall changes, and network settings. Employees may not install or download any software, either from the Internet or other sources. Only IT staff members are authorized to install software; users requiring assistance should contact the Help Desk.

Software Licenses

Only software licensed to the College and the University may be installed on any workstation. Unlicensed (pirated) copies of commercial software are expressly forbidden.

Backup Policy

Information Requiring Backup

All critical business information and applications on College servers are subject to back-up policy. Critical business information includes, but is not limited to, administrative data (financial, HR, admissions, etc.), faculty research, data related to grants and contracts, curriculum, student-related records, etc. Critical business applications include, but are not limited to, file servers, email servers, database servers, web servers, and special purpose application servers.

Backup Storage

All data that is backed up via the College of the Liberal Arts backup software is copied to tape media in two different locations (separate buildings) on two different tape library systems, one in each location.

After 30-60 days in the tape library, the backup tape media must then be moved to a third location offsite from the tape library systems, stored in a fireproof safe in a restricted area secured by a locked door. The offsite facilities must be a sufficient distance from the originating facility to escape a local disaster.

Transmission of Backup Data

All backup data is encrypted from the source to the target location, as an additional security measure backups of sensitive data is also encrypted in transit.

Backup Media at Rest

All data contained on backup media at rest is encrypted.

Backup Schedule

College File Server Data (Home, Departmental Data)

College file server home and departmental data is backed up daily and kept online for 30 days and offline for 485 days. The backup process is performed with sufficient frequency to support documented contingency plans.

College File Server Data (Research Data)

College file server research data is backed up daily and kept offline for 485 days. Due to the size of research data it is not practical to keep online backup copies of the data. The backup process is performed with sufficient frequency to support documented contingency plans.

College File Server Operating Systems

College file server operating systems are backed up daily and kept offline for 60 days. The backup process is performed with sufficient frequency to support documented contingency plans.

College Application Servers

College file server operating systems are backed up daily and kept offline for 60 days. The backup process is performed with sufficient frequency to support documented contingency plans.

Central E-mail Application and Operating System

College file server operating systems are backed up daily and kept offline for 60 days. The backup process is performed with sufficient frequency to support documented contingency plans.

College Server Security Event Logs

College server security event logs are backed up daily and kept online at least 30 days and offline 6 years. The backup process is performed with sufficient frequency to support documented contingency plans.

College Firewall Logs

College firewall logs are backed up daily and kept online for 14 days and offline for 6 years. The backup process is performed with sufficient frequency to support documented contingency plans.

Backup Integrity

Testing: Backups and Media

The computer data media used for storing proprietary information is of high quality and periodically tested to ensure that it can properly record the data. Used data media that can no longer reliably retain information is destroyed.

Testing: Recovery Procedures

The procedure by which data restoration is achieved is tested annually to ensure that data restoration from backups is achievable in a manner compliant with College policy.

Desktop Local Drive Backups

Employees must not store administrative information on local hard drives. The contents of local desktop hard drives are not backed up by the College and therefore should not contain administrative data. All faculty research data should be kept on College file servers to ensure the data is backed up.

Laptop Local Drive Backups

Employees must not store administrative information on local hard drives. The contents of local portable hard drives are not backed up by the College and therefore should not contain administrative data. All faculty research data should be kept on College file servers to ensure the data is backed up.

Personal Information Backups

The College will not backup personal information. Personal information includes, but is not limited to, pictures, movies, music, personal e-mail or email attachments, executable files, PDF documents, and zip files. These types of files must not be saved on College servers (such as your home H: drive or departmental share).

Media Handling, Sanitization, and Disposal Policy

Destruction

All College information will be securely destroyed after it is no longer needed.

Hard Drives (Internal or External)

Upon end-of-life all hard drives (internal or external) owned by the College and containing College data are sanitized meeting Department of Defense (DOD) standards.

Copier, Digital Sender, Multi-Function Copier/Fax and Printer Hard Drives

Upon end-of-life or returning a leased piece of equipment, all hard drives (internal or external to the device) owned or leased by the College and containing College data are required to be sanitized meeting Department of Defense (DOD) standards.

Other Removable Media

Upon end-of-life, all other forms of removable media (floppy disks, CDs, DVDs, tapes, etc.) containing College data will be physically destroyed rendering data irretrievable.

Media Handling Point of Contact

The IT Director is the central point of contact for all issues related to handling and disposal of College data.

Personnel Security Policy

Signed Acknowledgement of Understanding of Policy

All new employees must indicate their understanding of this site security policy by signing the College of the Liberal Arts Security Policy Manual User Agreement acknowledging that they understand and agree to subscribe to the policies within the manual. The signed acknowledgement forms are retained by HR.

Training & Awareness Policy

Security Awareness Program (SAP)

The University provides annual and ongoing security training and awareness that addresses the security needs of the faculty, staff, students, managers, and administrators. The program ensures that all persons responsible for network resources and the information contained therein, and all persons who access the network are aware of proper operational and security-related policy, procedures, and risks.

Security Reminders

The College of the Liberal Arts' technical support Web site will be utilized to publish regular reminders about information assurance and secure computing to all users. Changes to policy should be communicated via newsletter and/or e-mail.

EXCEPTIONS AND EXEMPTIONS

Exception to or exemptions from any provision of these policies must be approved by the College of the Liberal Arts Dean or designee, which will normally be the Associate Dean for Research and Graduate Studies. Similarly, any questions about the contents of this policy or the applicability of this policy to a particular situation should be referred to the Director of Administrative Services in the College of the Liberal Arts.