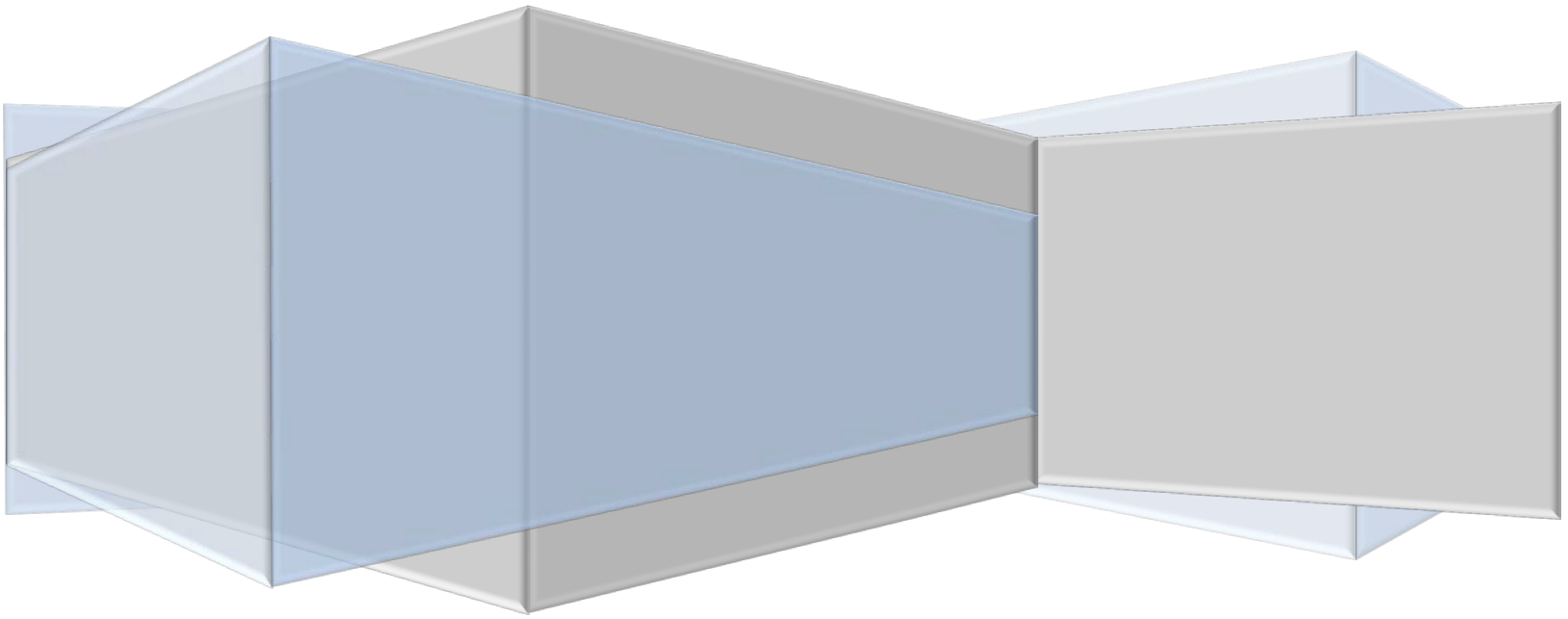
Date of Last Review: 05-04-2015

Information Systems Security Policies/Procedures

Student Affairs Information Technology

Northwestern University



Contents

1.0 Introduction

This document constitutes an overview of the Student Affairs Information Technology (SAIT) policies and procedures relating to the access, appropriate use, and security of data belonging to Northwestern University's Division of Student Affairs. The policies herein are informed by federal and state laws and regulations, information technology recommended practices, and university guidelines published by NUIT, risk management, and related units.

1.1 Purpose

This policy is intended to provide a basic understanding of the safeguards instituted by SAIT to protect Student Affairs data, and to serve as a guide to Student Affairs staff for conduct of business using technology resources. Where applicable, references are provided for relevant university policies, websites, and forms.

1.2 Scope

The policies laid out in this document apply to all departments within the Division of Student Affairs. Any person observing a violation of these policies must promptly notify their supervisor and one of the following units:

- SAIT - sa-help@northwestern.edu, (847) 467-7248
- NUIT - consultant@northwestern.edu, security@northwestern.edu, (847) 491-4357
- Ethics and Compliance – www.northwestern.edu/ethics, (866) 294-3545

Any request for exceptions to these policies can be submitted to SAIT using the contact information above. Requests will be reviewed in committee. Policy owners, data stewards, NUIT security staff, and other authorities may be contacted as necessary for consideration of the request.

This document and the policies to which it refers are reviewed on a periodic basis for currency, incorporation of new technologies, and accordance with NUIT policies.

1.3 Language

In order to be inclusive of all members of the Student Affairs community, "they" and "their" will be used throughout this document as a gender-neutral singular pronoun.

2.0 Definitions

Below are some definitions of key terms and abbreviations used in this document.

Term	Definition
A & AS	Audit and Advisory Services, the Northwestern office providing independent assurance and consulting relating to risk management, control, and governance processes.
Active Directory	A central identity management service developed by Microsoft for authentication and authorization services.
Certificate	An electronic document used to verify the identity of originators of data.
Certificate Authority	An authority in the network that issues and manages security credentials for message encryption.
Data Steward	The individual(s) responsible for the administration of access to subsets of information.
Encryption	The process of encoding messages to preserve the confidentiality and/or integrity of data.
Enterprise System	Any central system used as the only delivery platform for an essential service, often serving a broad constituency spanning organizational boundaries.
ERM	Enterprise Risk Management, a comprehensive, organization-wide set of processes and procedures used to document and manage risk.
Federated Authentication	An NUIT service that allows faculty, staff, and students to login to externally-hosted systems with their Northwestern NetIDs.
Firewall	Any hardware or software designed to examine network traffic using policy statements to block unauthorized access while permitting authorized communications to or from a network or electronic resource.
Firewall Ruleset	A set of policy statements or instructions used by a firewall to filter network traffic.
Host	Any computer connected to a network.
Host Firewall	A firewall application that addresses a separate and distinct host.
HTTP/HTTPS	Hypertext Transfer Protocol, the application protocol used for most data communication on the Web. HTTPS is a version of this protocol that uses SSL/TLS to provide encryption and secure identification of a server.
ISS/C	Information Systems Security/Compliance, the Northwestern office providing leadership and coordination in the development of policies, standards, and access controls for the safe-guarding of university information assets.

LDAP	Lightweight Directory Access Protocol, a protocol allowing user authentication against a centrally-maintained identity and password database.
Malware	Any malicious piece of software that threatens the confidentiality, integrity, or availability of data on a computer system or network.
NetID	A unique combination of letters and numbers created and managed by NUIT for use by staff as an electronic identity at Northwestern.
Network Device	Any physical equipment attached to the university network and designed to view, cause, or facilitate the flow of traffic within a network.
Network Extension	Any physical equipment attached to the university network designed to increase the number of available ports for network access.
Network Firewall	A firewall appliance attached to a network for the purpose of controlling traffic flow to and from single or multiple hosts or subnets.
NUIT	Northwestern University Information Technology, the central IT unit at Northwestern.
Portable Media or Devices	Any transportable object capable of containing data, including but not limited to cassettes, floppies, CDs, DVDs, SD cards, flash drives, zip drives, and external hard drives.
SAIT	Student Affairs Information Technology, the IT unit for Student Affairs and the owner of this policy.
SSL/TLS	Secure Sockets Layer and Transport Layer Security, two protocols used to authenticate servers and clients and to encrypt messages between the authenticated parties.
SSO	Single Sign-On, a service offered by NUIT for restricting access to websites or web-based applications via a single authentication service, requiring only one credential entry from users to gain access to all participating sites.
University Network	All network infrastructure and associated devices provided or served by the university.
Workstations	Any personal computer, including both desktops and laptops, but excluding tablets, PDAs, smartphones, etc.

3.0 SAIT Organization

3.1 User Services and Support

The User Services and Support team, which consists of full-time staff as well as part-time student employees, serves as a liaison between Student Affairs staff and NUIT and an initial point of contact for issues requiring assistance from other SAIT teams. In addition to these responsibilities, the team administers and provides technical support for all Student Affairs workstations and software, ensuring that division staff have the tools necessary to complete their jobs effectively and securely.

3.2 Infrastructure and Application Support

The Infrastructure and Application Support team administers the Student Affairs server environment and provides technical support for server-hosted applications used by Student Affairs staff. The team delivers secure and reliable access to Student Affairs data and systems, and works with vendors to implement new products and upgrades as necessary.

3.3 Application Development

The Application Development team supports the Student Affairs division by building innovative web/mobile application solutions for both staff and NU students that solve problems ranging from facilitating logistical workflow to reducing time delays during emergency situations. The team also provides technical support and training for use of the Cascade Content Management System for web content. In addition to these in-house responsibilities, SAIT's Application Development team is a strong campus advocate for recommended coding practices and web accessibility, providing presentations and training for the NU community.

4.0 Applicable Requirements

The requirements contained in this document are based on the following laws, regulations, and guidelines, and are tailored to meet the specific needs of the Student Affairs environment. Some of the regulations listed below are applicable only to certain types of data under SAIT jurisdiction.

4.1 Laws, Acts, and Regulations

Northwestern University Information Technology (NUIT) Policies

Available on the NUIT website at http://www.it.northwestern.edu/policies/.

Health Insurance Portability and Accountability Act (HIPAA) Security Rules/HITECH Act

HIPAA contains two separate sets of rules: the Security Rule and the Privacy rule. The Security Rule deals specifically with Electronic Protected Health Information (ePHI), which exists in numerous processing facilities on the NU campuses.

Family Education Rights and Privacy Act (FERPA)

Gives students access to their education records, an opportunity to seek to have the records amended, and some control over the disclosure of information from the records.

Illinois Personal Information Protection Act (PIPA), 815 ILCS 530/1

Requires universities and other data collectors to notify affected individuals whenever a breach of the security of the data collector's system occurs.

Gramm-Leach-Bliley Act (GLBA)

Requires financial institutions to provide their customers a privacy notice that details what data the company gathers about the client, where this data is shared, and how the company safeguards that data.

Payment Card Industry (PCI) Data Security Standard (DSS)

Establishes a consistent level of information security controls on credit card data to prevent credit card fraud.

4.2 Guidelines

National Institute of Standards (NIST)

Identifies the information security standards established by the US government.

Federal Information Security Management Act (FISMA)

Identifies information security requirements for contracts issued by the federal government, such as the National Institute of Health, and references the NIST guidelines for specific requirements.

Internation Organization for Standardization (ISO) Information Security Standards, 27002

Identifies internationally approved standards for information security, making it the most overarching IT requirement standard. These standards are the basis of the NUIT information security architecture.

5.0 Protection of Student Affairs Information

University data must be protected in a manner commensurate with its sensitivity and criticality, regardless of where it resides or what purpose(s) it serves. Student Affairs employees or persons with access to Student Affairs data shall not:

- Make unauthorized use or alteration of any information in files maintained, stored, or processed on university-owned resources, or permit anyone else to make unauthorized use or alteration of such information.
- Seek personal benefit or permit others to benefit personally from any confidential information that has come to them by virtue of their work assignment.
- Exhibit or divulge the contents of any record or report to any person except in the conduct of their work assignment and in accordance with university and departmental policies.
- Knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- Operate or request others to operate any university equipment for personal business.
- Divulge PINs, passwords, or other private ID information to university personnel or outside persons.

5.1 Information Classification

Classifying data provides a means by which the level of protection afforded to that data can be appropriately matched to its sensitivity and value. Classification is informed by the guidelines and regulations in the Applicable Requirements section above, but data owners may also recommend classifications based on special familiarity with the data.

NUIT outlines three categories of data classification: public, internal, and legally/contractually restricted. Unauthorized disclosure or use of internal and legally/contractually restricted data may expose the university to risk and may therefore require additional training for Student Affairs staff that work with that data.

Data Access Classification: http://www.it.northwestern.edu/policies/dataaccess.html
Sensitive Data in Contracts: http://www.it.northwestern.edu/policies/contractlanguage.html

5.2 Data Access Management

As a division within an institution of higher learning, Student Affairs is committed to being as open and unrestricted as possible without compromising the confidentiality, integrity, and availability of its information resources. Access to data will consequently be as broad as possible, consistent with the classification of the data, the roles and responsibilities of the user, and the user's level of training.

5.2.1 Access Authorization

To work as a unit, Student Affairs employees must have shared responsibility for university data. Department directors may grant, revoke, or change access authorization at will, and should be consulted where appropriate extent of access for supervisees is ambiguous.

Subject matter experts within individual departments are frequently responsible for granting access to business applications and should abide by the spirit of the access authorization policy delineated in this section when granting access to staff.

5.2.1.1 Eligibility for Data Access

All non-student staff are granted user logon rights to department workstations and administrator logon rights to their primary (and, where applicable, secondary) workstations. In addition, they are granted access to the default level of their departmental share. Access to any other privileged folders within the share, or administrator access to other department workstations, must be requested by an authorized department representative. In cases where a new staff member is replacing outgoing staff, data access permissions are matched as closely as possible.

To obtain eligibility for data access, staff may be required to sign Non-Disclosure Agreements.

NetID and Network Privileges: http://www.it.northwestern.edu/policies/acctprivs.html
Non-Disclosure Agreements Guide: http://www.it.northwestern.edu/policies/nda.html

5.2.1.2 Short-term Data Access Authorization

Student and temporary staff are granted administrator logon rights only to their designated workstation, and have no user logon rights to department workstations. Access to the share is limited to designated folders for student workers, and granted to temporary staff only as requested by an authorized department representative. Departments are required to provide SAIT with quarterly lists of outgoing short-term staff for removal of data access permissions.

5.2.1.3 Changing Data Access Authorization

Assumption of new or different duties often requires a change in an individual's access to university resources. All requests for authorization changes in a staff member's access to shared data must be approved by an authorized department representative.

5.2.1.4 Revoking Data Access Authorization

All cases of transfer, reassignment of duties, retirement, and separation from university service should be reported to SAIT immediately. Revocation of SAIT-controlled permissions to IT systems will be implemented on the departing staff member's final day of employment within Student Affairs by SAIT staff.

All NetIDs are subject to an automated expiration process driven by NUIT authoritative systems, but auto-expiration should be viewed as a delayed safeguard, not the primary means of deauthorization.

Data access authorization may be revoked at any time by department directors. SAIT should be notified of any staff whose authorization should be removed.

NetID Expiration: http://www.it.northwestern.edu/netid/expiration.html

5.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data

There are many cases in which data is shared between enterprise application systems and Local Management Information Systems (LMIS). It is important to document these instances of data sharing and the particular parameters of the data sharing agreement, including the data elements to be shared, under what conditions the data is to be provisioned, and the responsibilities and security needs associated with provisioning data to the requesting system. Such documentation lends structure to the implementation and maintenance of the data sharing agreement and protects against confusion in instances of personnel turnover. Undocumented or "handshake" agreements pose risks to the institution, particularly if sensitive or nonpublic data becomes available to unauthorized individuals or entities because the requesting system is not appropriately secured and/or is not implementing institutional policies regarding data access.

Student Affairs departments wishing to electronically share university data with application vendors or other external parties are required to consult SAIT before a method of data exchange is established. SAIT is responsible for working with these third parties to provide a secure means of data transmission.

Protocol for Exchange and Shared Responsibility for Institutional Data: http://www.it.northwestern.edu/bin/docs/ExchangeSharedResponsibilityData.pdf

5.2.2 Workforce Member Identification

Northwestern University employs a single identifier, created by a central identity management system operated by NUIT, for user authentication and role-specific access to university systems. This identifier, known as a NetID, is not to be confused with the seven-digit EmplID assigned to all students and employees. NetIDs are never reassigned or reused, and they and their associated passwords are the property of NUIT.

NetID: http://www.it.northwestern.edu/netid/overview.html

5.2.3 Workforce Member Authentication

Authentication of users to university systems is conducted via NetID and associated password. All activities occurring under a NetID are directly attributable to the owner of the NetID, and owners are personally responsible for those activities. As a key to university systems and resources, an employee NetID or other credentials should be guarded carefully and never shared with anyone.

In keeping with government regulations, Northwestern closely monitors how information is collected, stored, exposed, and used in its academic, research, and administrative processes. This information is housed in the LDAP Registry database, a subset of which is mirrored in the central Active Directory forest. This information is classified as Legally/Contractually Restricted, and access to it must be requested and granted for each application requiring its use.

Identity Services:
http://www.it.northwestern.edu/about/departments/itms/identity-services/index.html

5.2.3.1 Software Applications Authentication

NUIT makes available four integrated NetID authentication methods for use by software applications:

1. Web Single Sign-On (via SUN Access Manager) is the preferred authentication method for applications within the Northwestern network
2. LDAP version 3 (via SUN Enterprise Directory 5.2) is available by request only and is limited to specific application credentials at specific IP addresses
3. Microsoft Active Directory (via Windows Server)
4. Federated authentication (via Internet2 Shibboleth)

For existing applications that do not support these authentication methods, SAIT or a designated department member is responsible for creating secure user login accounts.

Regardless of the method of authentication, applications may have a need for additional information about users for data access authorization. Where a Student Affairs department member has not been designated for this role, SAIT is responsible for building user profiles in all applications it administers.

User Authentication Services: http://www.it.northwestern.edu/auth-svcs/index.html
Authentication Requirements for University Software Applications: http://www.it.northwestern.edu/policies/coordinate.html
Software Authentication: http://www.it.northwestern.edu/policies/softwareauth.html

5.2.3.2 Authentication for Services Outside of the University Environment

All services outside the university must be accessed through a web interface. Federated authentication is the preferred method for authenticating and authorizing users. NUIT will not expose any other authentication method outside of its network.

If federated authentication is not possible, then authenticated access should rely upon a secure session-key technology to designate a persistent session with the service point. Because session-key techniques must be coordinated, any aspect of a proposed software system or service that requires such accommodation must be brought to SAIT's attention for evaluation.

Northwestern does not export or bulk transfer identities, passwords, or personal information to third parties for authentication or any other purpose.

5.2.3.3 Password Construction Requirements

NUIT provides NetID password construction requirements for use by staff when establishing a new NetID password. These requirements are subject to change as technologies evolve.

SAIT is responsible for ensuring that applications not using NetID authentication enforce password construction requirements at least as stringent as those required for NetIDs. Where applications do not allow such enforcement, Student Affairs staff should create passwords that mirror these requirements.

Password Requirements: http://www.it.northwestern.edu/netid/password.html
NetID Management: http://nuvalidate.northwestern.edu

5.2.3.4 Password Management

NUIT uses a password aging system that requires users to periodically change their NetID passwords. NetID owners will receive several email reminders to change their passwords as the expiration date approaches. Passwords may be changed more frequently than required, but must be changed at least once within the defined period to avoid deactivation.

Passwords for applications that do not use NetID authentication should be set to expire within a defined period where possible. Prompts for password resets in these applications will appear at the time of user login an application-specific number of days prior to deactivation. In applications for which SAIT does not manage logons, the department staff member managing the application should enforce this policy. Where policy enforcement through an application is not possible, staff members are individually responsible for periodically changing their passwords at least annually.

Restoring Passwords: http://www.it.northwestern.edu/netid/resetguidelines.html

5.2.4 Shared Accounts

Some departments allow multiple staff members to share responsibility for departmental NetIDs, departmental email accounts, or other shared accounts requiring credentials for authentication. It is the responsibility of departments to change shared passwords as frequently as staff turnover dictates. To facilitate and track password resets and renewals, both the director of SAIT and a designated User Services and Support staff member should be owners on all requested departmental NetIDs.

Shared accounts must not be used to authenticate to the Northwestern network or to access data that is sensitive or otherwise subject to monitoring or logging of retrieval, modification, or deletion.

5.3 Confidentiality

The Northwestern network is owned and operated by the university for its own academic, research, and administrative purposes, and all transmissions over the Northwestern network are viewed and treated as private. While data and communications are considered confidential, use of the university network and computing resources is strictly by permission of the university, and confidentiality is not guaranteed. Under certain conditions and with specific approvals, data may be subject to review. SAIT may furnish any information on data use and abuse to NUIT upon request.

Data Privacy:
http://www.it.northwestern.edu/policies/privacy-issues.html http://www.it.northwestern.edu/policies/uccpolicy.html

5.3.1 Secure Handling of Social Security Numbers

Social Security Numbers may not be captured, retained, communicated, transmitted, displayed, or printed in whole or in part, except where required or permitted by law, and in accordance with the standards outlined in the Applicable Requirements section above.

Approved Uses of SSNs: http://www.it.northwestern.edu/bin/docs/ApprovedUsesAppB.pdf
Secure Handling of SSNs: http://www.it.northwestern.edu/policies/SSN_policy.html

5.3.2 Data Encryption

Encryption provides an enhanced level of assurance that data cannot be viewed by unauthorized parties in the event of theft, loss, or interception. Full disk encryption obscures all data on a system, including files, folders, and the operating system. The less physically secure a system is, the more appropriate it is to encrypt data.

Full disk and/or boot disk encryption may be combined with file/folder encryption in order to provide two layers of encryption to protect data in the event that the first layer is compromised. Individual or multiple files that are encrypted separately from the host operating system can be transmitted securely via email or stored in locations such as network shares or external harddrives.

SAIT makes uses of encryption software centrally hosted by NUIT and licensed per workstation. In addition to encryption software installation performed by default under the circumstances indicated below, Student Affairs staff may request installation on any university-owned workstation.

Data Encryption: http://www.it.northwestern.edu/policies/dataencryption.html

5.3.2.1 Devices

Desktops

Because stationary workstations such as desktop computers are frequently behind locked doors when not supervised, they enjoy greater security than many other devices. It is therefore SAIT policy to implement full disk encryption only on desktops that a) process data classified as Legally/Contractually Restricted or b) serve as primary machines for staff located in spaces that may be both publicly accessible and unsupervised at any point during the day.

Laptops

Mobile systems such as laptops are highly susceptible to theft or loss and frequently contain valuable data. SAIT implements full disk encryption on all laptops that a) serve as primary machines for staff or b) serve as secondary machines that contain data classified as Legally/Contractually Restricted.

Mobile Devices

Like laptops, mobile devices such as PDAs and smartphones allow users to exchange, transfer, and store university information outside of the office. The size and portability of these devices render them especially susceptible to theft or loss. Full disk encryption of mobile devices is not currently a viable option. SAIT recommends the use of standardized devices such as desktops and laptops for storing, transmitting, or processing data classified as anything other than Public. Any Student Affairs employees whose mobile devices contain such data—either through syncing of email, mobile application access, or download—are required to set a screen lock at the time of setup.

External Devices

External devices such as hard drives, DVDs, CDs, and USB flash drives can be encrypted in their entirety. SAIT strongly discourages the use of external devices to transport sensitive university data, but can

encrypt devices upon request from users where other means of data access are unavailable. Unencrypted devices should not be used for storage of any data not classified as Public.

5.3.2.2 *Disk Decryption*

SAIT maintains a separate encryption administrator account and password on all encrypted machines. This is a hedge against data loss, should a user forget their password, leave the university unexpectedly, or experience a hardware failure that renders the disk inaccessible. NUIT also provides a one-time use Whole Disk Recovery Token (WDRT) for encrypted machines to which neither the primary user nor SAIT staff are able to gain access.

5.3.3 Data Search Utilities

In order to protect sensitive data, it is first necessary to identify where the data is stored. SAIT may make use of NUIT-recommended data search utilities to locate sensitive data on Student Affairs workstations and network drives. Where necessary, data may be relocated or afforded additional protection appropriate to its level of sensitivity. Data stewards will be made aware of any such preventative or remedial measures.

Data Search Tools: http://www.it.northwestern.edu/policies/datasearch.html
Searching Character Strings: http://www.it.northwestern.edu/bin/docs/character_string_search.pdf

5.4 Data Integrity

Data integrity refers to the maintenance and assurance of the accuracy and consistency of date over its entire life cycle. The overall intent of any data integrity technique is to ensure that data is recorded exactly as intended and, upon later retrieval, is the same as when it was originally recorded. It is a critical aspect of the design, implementation, and usage of any system that stores, processes, or retrieves data. SAIT selects and implements security mechanisms such as data encryption to provide not only availability and confidentiality, but also integrity of data, whether it is at rest, in use, or being transmitted.

5.5 Data Backup and Recovery

In the event of hardware failure, data corruption, or data loss, it is important to have a backup of university data outside of the workstation or server on which it is normally stored. As part of its commitment to the protection of mission critical data, SAIT uses a cost-effective and secure-hosted data backup solution shared among many of the university's schools and departments. This solution is licensed per seat and includes a limited amount of storage space, with expansion possible for an additional fee.

All encrypted workstations should include backups to protect against data loss in the event that decryption is not possible.

Data Backup: http://www.it.northwestern.edu/security/backup/
Central Data Backup Solution: http://www.it.northwestern.edu/dss/backup-service/index.html

Workstations

Except where encryption requires backup services, Student Affairs workstations are backed up on a case-by-case basis by request from department staff. Picture and music storage is not included by default in these backups, but staff can request at the time of installation that university-relevant data of this type be backed up. Staff can also control their own backup directories through the user interface on their machines. Where an inordinate amount of storage space is being used by a single staff member, SAIT may adjust backup settings to exclude non-university data stored on university-owned machines.

Servers

Server Backups

Student Affairs servers that are created and hosted by NUIT at the Datacenter are backed up according to NUIT procedures, which can include VM snapshots, versioning, and Volume Shadow Copy.

For all SAIT-hosted and NUCloud-based servers, backups are made with the centrally hosted backup service indicated above. Directories to back up are decided on a server-by-server basis.

On-Site Backups

The centrally hosted service backs up to its own servers to a secure off-site location. As an additional precautionary measure, SAIT requires servers to be backed up to its own in-house hard drives. Hard drives are swapped at the end of every week, and the inactive backup drive is stored in a padded, moisture-free enclosure within a fireproof safe.

Off-Site Backups

SAIT benefits from NUIT's off-site data storage service, with pickup and drop off provided by the vendor. To meet data protection audit requirements, a media rotation of grandfather – father – son is generally followed. Departments may negotiate a media retention period; fees incurred are based upon the frequency of the pick-up/drop-off service and the number of containers required.

Off-site Data Protection Guidelines: http://www.it.northwestern.edu/policies/storageguide.html

Database Backups

SAIT uses scheduling agents to write full database backup files to disk at on a staggered schedule each day. These files are included in the directories slated to back up to an off-server location via one of the methods listed above.

Data Retention

Departments are responsible for communicating their data retention needs to SAIT. These needs should be informed by laws and regulations pertaining to the data classification and by business requirements known to the department.

The NUIT Datacenter is not responsible for enforcing data retention, either on tape or digitally on the centrally hosted backup solution. SAIT ensures that all data whose lifecycle is not complete is stored in a secure manner and is actively backed up according to data backup policies.

5.6 Data/Equipment Destruction

Once data has reached the end of its lifecycle, it must be erased in a manner commensurate with its sensitivity. Deletion of files and/or reformatting of a drive are in most cases insufficient for data destruction. Machines that are leaving the university, either through services listed below or some other method, must have their hard drives sanitized with a three-pass binary wipe, which writes zeroes, ones, and then pseudo-random data over existing data. SAIT uses both open source and off-the-shelf products for this process.

For computer equipment itself, University Services offers a service to formally dispose of and reuse university-owned machines and peripherals. This no-charge service is designed to help meet security and EPA regulations for equipment disposal. Disposal of equipment with inventory tags (or cost exceeding $5000) must be reported to the Accounting Services Equipment Inventory Coordinator. For equipment acquired using federal funds, approval for disposal must be obtained from Accounting services for Research and Sponsored Programs (ASRSP).

SAIT schedules all workstation, server, and other hardware surplus disposal for Student Affairs. Departments should turn over equipment that is no longer required to SAIT for data removal and disposal. Equipment that is still functional may be repurposed within the division.

Disposal of NU Computers: http://www.it.northwestern.edu/policies/disposal.html
eCycling: http://www.northwestern.edu/uservices/office/computer/staff.html
ASRSP: http://www.northwestern.edu/asrsp

Workstations

SAIT is responsible for securely wiping the drives of machines slated to leave the university. In addition to undergoing a multi-pass data overwrite, drives that have stored Legally/Contractually Restricted data and are leaving the university are physically destroyed.

SAIT also performs a multi-pass wipe on workstations that have stored Legally/Contractually Restricted data and are being repurposed in another area of the division.

Servers

SAIT-hosted servers containing any category of data undergo a multi-pass wipe before physical disposal. Server drives that have hosted Legally/Contractually Restricted data are also physically destroyed after data overwrite.

Data occasionally needs to be removed from servers without a full server wipe—e.g. if information is mistakenly stored on the incorrect server, or a file is decrypted when it should have remained encrypted. SAIT uses a sensitive data removal program to securely delete discrete segments of data from servers.

Physical Media

CDs, DVDs, or tapes containing data or software must be physically destroyed before disposal. Destruction of discs can be dangerous if done improperly, as discs rarely break cleanly or predictably,

and fragments are often jagged. Although Student Affairs personnel may physically destroy discs on their own, CDs and DVDs can also be turned in to SAIT for disposal.

Paper

University data stored in paper form should be shredded prior to disposal. Departments are responsible for ensuring the destruction of their paper data.

Shredding Vendor: http://www.northwestern.edu/uservices/purchasing/vendors/secure/cintas-document.html

6.0 Information Systems Acceptable Usage

Student Affairs staff or persons with access to SAIT computing services shall abide by the IT Computing Services guidelines. All violations of these guidelines must be reported to the Director of SAIT immediately.

Appropriate Use of Electronic Resources: http://www.it.northwestern.edu/policies/electronic-resources.html
Standards of Business Conduct: http://www.northwestern.edu/audit-and-advisory/docs/standards-of-business-conduct.pdf

6.1 Standard Equipment Configuration

Workstation Configuration

Workstations, including both desktops and laptops, are frequently subjected to attempts to exploit system and application vulnerabilities. Student Affairs division staff should abide by the following guidelines regarding workstation configuration.

Workstation Security Recommendations: http://www.it.northwestern.edu/policies/desktop_security.html

Staff Responsibilities

Though SAIT handles initial setup and configuration, staff are granted sufficient access to customize their workstations. The guidelines below should be followed by staff at all times.

- Users must not tamper with settings to prevent automatic updates to security software, operating systems, and other non-university-hosted applications (Microsoft, Adobe, Java, etc.).
- Each user should have a separate workstation login account unless shared accounts are specifically authorized by SAIT. No additional user accounts should be created.
- Workstations should have the native operating system firewall activated.
- Installation of toolbars and other bloatware should be avoided.
- All instances of unfamiliar application prompts or error messages should be reported to SAIT.

SAIT Responsibilities

In addition to the guidelines under Staff Responsibilities, SAIT employees should adhere to the following guidelines.

- Where possible, security policies should be set at the server level and applied to workstations.
- Antivirus/Endpoint security software should be installed on all PCs.
- All security software, operating systems, and non-university-hosted applications (Microsoft, Adobe, Java, etc.) should be set to check for and apply updates automatically.
- Guest accounts should be disabled, and an administrator account for IT use should be established.
- All compromised workstations should be wiped and rebuilt from scratch.

- Broadly, workstations should start from a position of security and have services opened up as necessary.

Server Configuration

In addition to the recommendations for Workstation Configuration listed above, SAIT staff should follow further guidelines for server configuration:

- All privileged account read and write access should be audited.
- Software and OS patches should be applied automatically only if controlled by a central update server; otherwise, patches may be applied on a delay as they are vetted.
- Unused services should be disabled.

Server Security Requirements: http://www.it.northwestern.edu/policies/serversecurity.html

Single- and Multifunction Devices

Both local and networked devices such as printers, scanners, copiers, and faxes can be targeted for misuse. Student Affairs division and IT staff should abide by the following guidelines for use of single- and multifunction devices.

Networked Devices: http://www.it.northwestern.edu/policies/networked-devices.html

Staff Responsibilities

Though SAIT handles initial setup and configuration of devices, staff are granted sufficient access to customize settings for their business process. The recommendations below should be followed by staff at all times.

- Where department codes are used for authentication to printers and other devices, codes should not be shared with unauthorized users, even for temporary device usage.
- Administrator configurations such as network and user access settings should not be reconfigured without SAIT involvement.

SAIT Responsibilities

In addition to the recommendations under Staff Responsibilities, SAIT employees should adhere to the following guidelines. Single- and multifunction devices are capable of varying levels of configuration; all guidelines should be applied as possible according to the spirit of the security policy.

- Secure administrator passwords should be set on devices to defend against attacks and prevent reconfiguration by unauthorized users.
- Access control lists (ACLs) should be configured to allow connection only from the requisite subnets. Access from wireless and VPN networks may be allowed at the discretion of SAIT and the department responsible for the device.
- FTP, SNMP, and Telnet access should be disabled where not required.
- Appletalk, Netware, and other protocols or services that are not required should be disabled.

Mobile Devices

Mobile devices such as PDAs, pagers, tablets, and phones are increasingly used to transmit or store data, and are consequently exposed to an increasing number and sophistication of threats of compromise from malware, theft, and loss. As Northwestern is a BYOD-friendly workplace, the following guidelines provide some security for data that passes through these devices.

- Devices and apps should be kept up-to-date.
- Devices connected to Northwestern's Microsoft Exchange email servers must be secured with a screen-lock PIN.
- Devices storing data classified as Internal should be secured with a screen-lock PIN.
- Mobile devices should not be used to store Legally/Contractually Restricted data.

Mobile Device Security: http://www.it.northwestern.edu/policies/mobile-devices.html
http://www.it.northwestern.edu/hardware/iphone/iphone-collab.html

Portable Storage Devices

Portable storage devices such as CDs, DVDs, thumb drives, and external hard drives are frequently used to transmit or store data. The size and mobility of these devices render them particularly susceptible to theft and loss. The following guidelines lower the probability of compromise of data on such devices.

- Devices should be stored securely when not in use.
- Unencrypted devices should not be used to store Internal or Legally/Contractually Restricted data.

6.2 Personal Computer Configuration

Because SAIT personnel do not configure or regulate the use of personal computers, these devices can pose a security threat to university-owned workstations and networks if used for work purposes. The following guidelines should be followed for university data access on personal machines.

- Antivirus software should be installed and active on personal computers that handle university data or connect to the university network. Northwestern has allocated licenses for installation of antivirus protection on personal computers to encourage adherence to this policy.
- Data classified as Internal or Legally/Contractually Restricted should not be manipulated or stored on personal computers. SAIT provides remote access to staff workstations as required to ensure that staff can access and alter sensitive data without transferring it off of protected devices and/or networks.

6.3 Software

6.3.1 Patches

It is important to identify and install relevant patches and system updates to ensure the ongoing functionality and security of systems and applications. Where available, it is recommended that staff who have downloaded software set the automatic software update notification feature.

Patches to SAIT-hosted applications must be specifically requested by departments and are not automatically applied by SAIT except in cases where an important security update has been specifically communicated to SAIT staff. Because all changes to application code can introduce threats to data integrity and application functionality, departments requesting application updates should note the desired features or bug fixes included in the update that justify this risk.

6.3.2 Licensing

It is university policy that no member of the Northwestern community engage in any activity that violates federal, state, or local laws with respect to intellectual property rights or the terms of software license agreements. This policy applies to all computer software owned by or licensed to the university, as well as computer systems or hardware owned or operated by faculty, staff, and students.

Under the law, computer software (programs and computer-based information) is copyrighted intellectual property unless explicitly declared to be in the Public Domain. Licenses sold for software generally permit the purchaser to copy the software in specified ways in order to use it, including making a backup disk, copying onto a hard disk, or copying into memory on a computer. They also usually restrict simultaneous use by more than one person or use on more than one computer. Generally not granted is a right to receive and use unauthorized copies of the software or make copies of the software for others.

Software users must not:

- Make software available for others to use or copy in violation of that software's license agreement.
- Install, nor direct others to install, illegal or unlicensed copies of computer software onto any university-owned or operated computer system. SAIT conducts periodic reviews of computer systems for software installations to help ensure compliance with licensing agreements, copyright regulations, and university policy.
- Make copies of or make available on the network copyrighted material, including but not limited to software programs, music files, video files, digital images, radio and television broadcasts, and written text works, unless permitted by a license, consent of the copyright owner, or a fair use limitation under copyright law or the Digital Millennium Copyright Act (DMCA), as when copies are made by a library or archive for preservation purposes.

Copying Software: http://www.it.northwestern.edu/policies/software.html

6.3.3 Reuse

In general, Microsoft licenses its Windows operating system to the processor and motherboard of the workstation with which it is shipped. Disks that have been wiped may have the original Windows OS reinstalled before a workstation is redeployed to another division or leaves the university.

Any software purchased by departments through NUIT's site-licensed program is removed from outgoing workstations. If permitted by the software licensing agreement, it may be redeployed within the division.

6.4 Email

NUIT provides faculty and staff email service after NetID activation. All non-student staff are provided with centrally hosted Microsoft Exchange @northwestern.edu accounts, but optional Google-hosted @u.northwestern.edu accounts may be requested.

Cost of operations and equipment, performance of individual accounts, and overall server performance are influenced by disk storage use. Storage on individual accounts is limited, and a series of warning messages will be sent as accounts approach the storage limit. As storage limits are approached, staff are responsible for contacting SAIT for assistance in archiving old emails and removing them from the server. Additional space may also be requested from NUIT. Under no circumstances should email be forwarded to private accounts for extra storage.

Email is particularly susceptible to a host of adversarial activities, including attempts to steal user information or install malicious software on user machines. Northwestern's email services offer a system for scanning and filtering junk email and identifying phishing attempts, viruses, and malicious high-risk attachments sent to the University community. Any suspicious emails should be forwarded to SAIT or NUIT.

Email Accounts: http://www.it.northwestern.edu/accounts/email/index.html
Policy for Electronic Resources: http://www.it.northwestern.edu/policies/electronic-resources.html
Quotas: http://www.it.northwestern.edu/policies/inspool.html
Email Defense: http://www.it.northwestern.edu/security/eds/index.html

7.0 Network Security

The information technology environment at Northwestern can be described as layers of function around a core of central systems and university data warehouses. The Northwestern computer network that ties all this together consists of a campus-wide backbone network, local area networks, and many shared workstations, servers, and other networked devices.

7.1 Network Service Eligibility

The following groups are identified as eligible to receive information systems network services from NUIT. Any applicant for network services not described below should be referred directly to the vice president for information technology or a designee, who will coordinate a decision on that particular case.

- **Students:** All full-time undergraduate and graduate students, as well as medical residents, without restriction. Part-time students and continuing education students may receive network privileges subject to the policy guidelines of their school.
- **Faculty:** Full-time faculty without restriction. Part-time faculty, faculty with temporary or cyclical appointments, visiting faculty, contributed-service faculty, and instructors may receive network privileges subject to the policy guidelines of their school.
- **Staff:** All regular, non-faculty university employees without restriction.
- **Temporary employees, visitors**: temporary employees may receive network privileges at the request of the employing department. Documentation is required.
- **University organizations**: Departments, committees, and other logical focal points of business communication within the university may receive network privileges to conduct their business, especially as it applies to communicating officially outside of the university. Access should be confined to a minimum number of users. Documentation is required.
- **Student organizations**: Student organizations recognized by the Associate Student Government may receive an alias. Documentation is required.
- **Primary affiliates**: Faculty, staff, and students of some affiliate organizations may receive network privileges without restriction. Documentation may be required.
- **Secondary affiliates**: Faculty, staff, and students of other affiliate organizations may receive network privileges as granted by an established administrative process between the affiliate and the university.

7.2 Network User Rights

Members of Student Affairs can expect certain rights as they use the network and its services.

- **Intellectual Freedom:** Northwestern University is a free and open forum for the expression of ideas, including viewpoints that are strange, unorthodox, or unpopular. The university network upholds this principle: network administrators place no official sanctions upon the expression of personal opinion on the network. However, such opinions may not be represented as the views of the division of Student Affairs or the university as a whole.

- **Safety from Threats:** While unwanted or unsolicited contact cannot be controlled on the network, network users who receive threatening communications should bring them to the attention of University Police. Electronic threats are taken as seriously as voiced or written threats, consistent with university policy.
- **Privacy:** Data files and messages traversing the university network are not private communications. Northwestern reserves its right, as owner of the network and the computers in question to examine, log, capture, archive, and otherwise preserve or inspect any messages transmitted over the network and any data files stored on university-owned machines. All members of the community must recognize that electronic communications are by no means secure, and that during the course of ordinary management of computing and networking services, IT staff may inadvertently view user files or messages. In addition, if a user is suspected of violations of the responsibilities as stated in this document, that user's privacy is superseded by the university's requirement to maintain the network's integrity, protect the rights of all network users, and promote respect for applicable laws and applicable license provisions. Should the security of a computer be threatened, user files and messages may be examined under the direction of the vice president & chief information officer, the associate vice president for cyber infrastructure, or the director of SAIT.

Network Privacy: http://www.it.northwestern.edu/policies/privacy-issues.html

7.3 Network User Responsibilities

Network users are expected to live up to the responsibilities that come with the privilege of network access. Knowingly violating a network responsibility may result in the suspension of network access for users or groups of users. Depending on the seriousness of the violation, it may be referred through the university's disciplinary procedure process. Violations of federal or state laws may also result in referral to the appropriate legal authority.

- Users are responsible for their NetID and all computer accounts that are assigned to them. Users may not give anyone else access to their NetID or computer accounts, use a NetID or a computer account that was not assigned to them, or try in any way to obtain a password for another user's NetID or computer account.
- Users may not misrepresent themselves or their data on the network.
- Users are responsible for the security of their passwords. This includes changing passwords on a regular basis and keeping them private.
- Users must not use Northwestern's network resources to gain or attempt to gain unauthorized access to remote computers.
- Users must not deliberately perform an act that will seriously impair the operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the high-speed backbone network, blocking communication lines, or interfering with the operational readiness of a computer.

- Users must not run or install on any of NU's computer systems a program—including but not limited to viruses, Trojan horses, and worms—that could result in eventual damage to a file or computer system.
- Users must not attempt to circumvent data protection schemes, exploit security loopholes, or interfere with standard technical measures that identify and protect the rights of copyright owners.
- Users must abide by the terms of all software licensing agreements and copyright laws.
- Users must not deliberately perform acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of other users. Any person operating a network-intensive application or a defective computer that overloads university networks will be notified and steps will be taken to protect the overall network. This may include disconnecting the offending computer system from the university network until the problem is resolved. If the condition is an imminent hazard to the university network, disrupts the activities of others, or violates applicable law, then the offending computer system or the subnet to which it is attached may be disconnected without prior notice.
- Users must not place on any university-owned computer system information or software that infringes on the rights of another person or gives unauthorized access to another computer account or system.
- Users must not attempt to monitor another user's data communications, nor may they read, copy, change, or delete another user's files or software without permission of the owner.
- Users must not use university computing and network resources for commercial purposes. Resources are provided solely to support the mission of the university.
- Users must adhere to federal, state, and all other applicable regulations when making information available to others on the university network. The content of any such information is the sole responsibility of said users, and they will be liable for any violations of laws, regulations, or university policies.

All university computing and networking facilities are provided for use by faculty, staff, and students for relevant academic, research, or administrative pursuits. Private use must be approved in advance in keeping with policies expressed in the Northwestern University Employee Handbook. Any network traffic exiting the university is subject to the acceptable use policies of the network through which it flows, as well as to the polices listed above.

Continued violations of system and network policies will be referred to the appropriate office for discipline. Sanctions may include fines, restitution of funds, termination of computer or network access, probation, suspension, separation, or exclusion from the university. SAIT or NUIT security officers should be notified about violations of copyright laws or of these policies, as well as about potential loopholes in the security of any computer systems and networks at Northwestern.

Network Rights and Responsibilities: http://www.it.northwestern.edu/policies/responsibilities.html

7.4 Firewalls

Firewalls are typically categorized as either network or host. A network firewall is a device attached to a network for the purpose of controlling access to single or multiple hosts or subnets. A host firewall is an application that controls network access to an individual host. Both types of firewalls can be and often are used jointly, as the redundancy of controls provides additional security in the event of a compromise or failure of one.

Firewall Configuration: http://www.it.northwestern.edu/policies/firewall.html

7.4.1 Necessity for Firewalls

Both a network and a host firewall are:

- Required in all instances in which electronic equipment is used to capture, process, or store data classified as Legally/Contractually Restricted and the equipment is accessible via a direct or indirect Internet connection.
- Recommended in all instances in which electronic equipment is used to capture, process, or store data classified as Internal or Public and the equipment is accessible via a direct or indirect Internet connection.

In addition, a host firewall is recommended for any individual host with access to the Internet.

All installations, implementations, and modifications of a network firewall and its configuration and ruleset are the responsibility of the authorized NUIT firewall administrator, with the exception of ruleset maintenance performed by SAIT. All installations, implementations, and modifications of a host firewall and its configuration and ruleset are the responsibility of SAIT and should not be performed by division staff.

7.4.2 Installation of Firewalls

All network firewalls installed and implemented must conform to the current standards as determined by NUIT. Unauthorized or nonstandard equipment is subject to immediate removal, confiscation, and/or termination of network connectivity without notice.

NUIT requires a properly executed Risk Acceptance Agreement before a business unit is permitted to assume the management of a network firewall ruleset. SAIT has established such an agreement, and manages network firewalls for division subnets.

7.4.3 PCI Firewall Requirements

Any university entity operating under an e-merchant license is required to have properly configured firewalls in place to protect credit card data and comply with Payment Card Industry/Data Security Standards (PCI/DSS). NUIT will not operate any firewalls installed for the purpose of PCI/DSS compliance. Student Affairs departments who wish to support credit card transactions should contract with a PCI-compliant vendor to operate network equipment that falls within PCI/DSS scope and requirements. SAIT will provide technical guidance and coordinate the deployment of required equipment with NUIT and the vendor.

7.5 Workstation and Network Access

In addition to the security precautions listed in the Workstation Configuration section above, the following access controls should be implemented on workstations to regulate access to the Northwestern network.

7.5.1 Logging In

SAIT requires individual login accounts on all desktops, laptops, and applicable mobile devices. Shared computer logins are discouraged except where staff turnover is high enough to make maintenance of permissions impractical. All workstations include a local administrator account for SAIT use.

At the server and application levels, SAIT requires individual local or network login accounts for each staff member where practical, as well as a local administrator account for emergency use.

7.5.2 Login Attempts/Lockout

Limiting the number of login attempts is an effective means of protection against automated password cracking attacks. Where a workstation is deemed vulnerable to such attacks, a login attempt counter should be instituted. Lockout policies can help to further reduce the number of attempts and time required to reach that number.

SAIT enforces a lockout policy on any workstations and applications (where possible) that provide access to Legally/Contractually Restricted data.

7.5.3 Inactivity

Inactivity logoff is another measure to reduce the likelihood of unauthorized access to workstation accounts and/or the Northwestern network.

SAIT enforces an inactivity logoff on all Student Affairs workstations and applications (where possible), with short session log-off timers on workstations and applications that provide access to Legally/Contractually Restricted data.

7.6 Network Time Protocol

Network Time Protocol (NTP) is used to keep a computer's internal clock synchronized with a central source. Having accurate time is critical for system administration and security. SAIT uses the Northwestern-provided on-campus NTP service time.northwestern.edu for all servers not joined to a domain.

NTP: http://www.it.northwestern.edu/network/ntp/index.html

7.7 Malware

Aside from on-disk scanning, antivirus software also provides active protection from network threats. It is critical that every Student Affairs staff member maintain an up-to-date version of the university-provided antivirus software on all Windows workstations that will be accessing the Northwestern network, whether university- or staff-owned. Antivirus firewalls may be omitted where they interfere

with the functioning of applications, provided host and/or network firewalls are in place. Any changes to antivirus software configuration by a Student Affairs staff member must be approved by SAIT.

Symantec Anti-virus: http://www.it.northwestern.edu/software/sav/index.html

7.8 Server Network Access

In addition to the security precautions listed in the Server Configuration section above, the following network access controls should be implemented on servers.

- Firewall exceptions should be disabled or restricted to the minimum scope required for business processes.
- No open, non-authenticated file sharing may be enabled.

Server Security: http://www.it.northwestern.edu/policies/serversecurity.html

7.9 Transmission Security

The need for parties to communicate securely over an insecure medium such as the Internet is served by processes such as the Public Key Infrastructure (PKI) framework. PKI frameworks utilize public-key cryptography and digital certificates in order to provide integrity and/or confidentiality to communications between parties. Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient in order to ensure delivery without eavesdropping, interception, or forgery. Trusted authorities, known as Certificate Authorities (CA), sign and distribute certificates for use by entities that need to assure identities and establish encrypted communications. Northwestern participates in the InCommon certificate program, which entitles NUIT to issue unlimited Secure Sockets Layer (SSL) certificates that help assure the integrity and confidentially of encrypted communications. This program allows SAIT to obtain SSL certificates at no cost.

In accordance with Northwestern policy, SAIT ensures that all Student Affairs systems, applications, appliances, or sites that use the NetID/password combination for purposes of authentication, or that transmit/receive data classified as Legally/Contractually Restricted:

- Employ secure Sockets Layer (SSL), Transport Layer Security (TLS), or their equivalent cryptographic protocols for authenticating and establishing identities and maintaining encrypted communications channels between endpoints;
- Use a Secure Hypertext Transport Protocol (HTTPS) connection based on server-side SSL certificates signed by a recommended trusted third-party certificate provider;
- Safeguard application and database servers behind an approved firewall

Server Certificates: http://www.it.northwestern.edu/policies/server-cert.html
SSL Certificates: http://www.it.northwestern.edu/security/ssl-certificate/
Encryption of Data in Transit: http://www.it.northwestern.edu/policies/dataencryption.html

7.10 Remote Access

Access to devices on the Northwestern network may be required outside of normal business hours. There are two security-related steps to accessing workstations and other Northwestern resources remotely: connection to the Northwestern network and connection to the desired device.

7.10.1 Remote Network Access

Northwestern provides two means of secure access to the university network from off campus locations.

7.10.1.1 VPN

A Virtual Private Network (VPN) establishes a secure and authenticated pathway by encrypting all network traffic and giving the appearance that the user is on the local network, regardless of geographic location. The VPN connection is an extension of the university network and subject to the university's policies. Connections are automatically ended twelve hours after initiation for service and security reasons.

VPN access is available by default to all members of the Northwestern community who possess a NetID. Student Affairs staff may configure VPN access on their workstations or request SAIT assistance in doing so.

VPN: http://www.it.northwestern.edu/oncampus/vpn/

7.10.1.2 SSL VPN

A Secure Sockets Layer VPN (SSL VPN) can be used as an alternate means of remote access to the network. Like the standard VPN, SSL VPN establishes a "secure tunnel" to the network; however, this protocol achieves a higher level of compatibility with client platforms and configurations. In particular, it is intended to provide authenticated/encrypted access to restricted resources such as servers or centrally-accessed systems and applications. SSL VPN can be accessed through a web proxy or a local client, and control to resources is determined by LDAP directory group membership.

SSL VPN groups are established by NUIT, and group membership is managed by SAIT. Department heads interested in establishing departmental access to a system should contact SAIT for SSL VPN group creation.

SSL VPN: http://www.it.northwestern.edu/oncampus/vpn/sslvpn/

7.10.2 Remote Desktop Access

Once remote access to the Northwestern network has been established, workstations on the network may be accessed using Remote Desktop Protocol (RDP). Department heads should notify SAIT of any staff members who require remote access to workstations, as SAIT maintains strict control over these permissions.

Remote Desktop Client for Windows and Microsoft Remote Desktop Client for Mac are the only SAIT-supported applications for RDP access. Staff should not use third-party software to circumvent access controls, as these pose a security threat to systems.

7.11 Wireless Access

In response to the increasing and widespread interest in wireless networking from individuals and departments, NUIT has developed wireless networking services that provide the same high level of management and reliability provided by the present campus wired network standards. Wireless access points are available throughout campus to anyone with a valid NetID. A guest wireless network allows limited Internet connectivity for visitors without NetIDs via network registration.

Because wireless networks, along with many other communications devices, operate on both FCC-licensed and -unlicensed bands, it is not unusual for one piece of equipment to interfere with another, causing a degradation in service quality. In addition, wireless networks are inherently less secure than wired networks. Installation, engineering, maintenance, and operation of wireless networks on any property owned or tenanted by the university are the sole responsibility of NUIT. Any independently installed wireless communications equipment is prohibited and is subject to removal from service and confiscation without notice.

Wireless Network: http://www.it.northwestern.edu/oncampus/wireless/
Wireless Access Points: http://www.it.northwestern.edu/oncampus/wireless/locations.html
Guest Wireless: http://www.it.northwestern.edu/oncampus/guest-wireless/index.html

7.12 Secure Web Applications and Coding

Secure coding is the practice of writing code for systems, applications, and web pages in such a way as to ensure the confidentiality, integrity, and accessibility of data related to those systems. An increasing number of targeted attacks focus on application vulnerabilities, making secure coding and attention to recommended practices more and more important.

SAIT helps ensure that its applications are developed and maintained with a minimum exposure to known security vulnerabilities by participating in the Information Security Vulnerability Management and Web Application Assessment Programs provided by NUIT's Information Systems Security/Compliance team (ISS/C). For web application assessments, ISS/C uses an automated vulnerability assessment tool designed to scan applications and apply attack algorithms to locate vulnerabilities and determine their severity. SAIT developers also consult the OWASP Top Ten or CWE/SANS Top 25 lists, which details the most common software security vulnerabilities, as well as basic methods to protect against them.

Services delivered from mixed or off-campus host configurations must be authenticated via NetID and password unless exempted by NUIT. On-campus or mixed host configurations must be authenticated via the NUIT Web SSO facility.

OWASP Top Ten: http://www.owasp.org/index.php/OWASP_Top_Ten_Project
CWE/SANS Top 25: http://www.sans.org/top25-software-errors/
Web Applications: http://www.it.northwestern.edu/policies/webapps.html
Web Assessments: http://www.it.northwestern.edu/security/vulnerability.html
Authentication: http://www.it.northwestern.edu/policies/coordinate.html

7.13 Accountability

7.13.1 Activity Monitoring

It is the policy of Northwestern to treat all transmissions over the Northwestern network as private; however, the use of the university network and computing resources is strictly by permission of the university, and confidentiality is not guaranteed.

All users of Northwestern's computing and network resources must be aware that privacy of electronic communication and/or stored data files may be routinely compromised by:

- Inadvertent capture of transmission contents during network performance monitoring or troubleshooting
- Uncovering of transmission contents in computer memory within the store-and-forward systems that move data through the network
- Other maintenance activities that trap, copy, archive, or otherwise unintentionally preserve portions of messages within the university networks

If SAIT or NUIT inadvertently discover messages or data files within its network that leads it to suspect the presence of illegal activities or activities that violate Northwestern policies, it will be free to use that discovered information to pursue investigations or inform the appropriate authorities.

7.13.2 Computer, System, or Network Monitoring

Northwestern reserves the right to take whatever steps are necessary to investigate possible network security threats or suspected violations of university regulations, or to assist appropriate authorities to investigate suspected illegal activities. On rare occasions, and with the approval of an IT director, files belonging to individuals and/or communications between individuals may be captured, logged, and examined.

8.0 Physical Security

Physical security encompasses the security of facilities, personnel, and IT equipment. Personnel safety is primarily handled by the University Police (UP), while the security of facilities is under the purview of Facilities Management (FM). SAIT uses resources provided by UP and FM to ensure the physical security of IT equipment.

University Police: http://www.northwestern.edu/up/
Facilities Management: http://www.northwestern.edu/fm/

8.1 Facility Security Plan

8.1.1 Physical Access Controls

Access to Student Affairs facilities containing IT equipment is regulated via standard metal keys, Marlock keys, RFID fobs, or some combination of these. Locks and keys are controlled and distributed by FM, and records of entry are retained in FM databases.

Access to SAIT server rooms is restricted to staff with a business need for entry.

Entry Control: http://www.northwestern.edu/fm/services/operation-and-maintenance-services/locks-and-keys.html

8.1.2 Power and Environmental Controls

FM is in charge of maintaining HVAC, fire protection, and power for all facilities. SAIT maintains uninterruptible power supplies in all server rooms and for select IT equipment around campus, as business requirements dictate. SAIT also regulates and monitors server room environmental elements, such as temperature and humidity, to ensure safe storage and performance. All cabling feeds into server rooms are protected with firestops.

Facility Engineering: http://www.northwestern.edu/fm/services/operation-and-maintenance-services/engineering.html

8.1.3 Facility Maintenance Records

Maintenance records should be kept by departments responsible for upkeep of facilities.

8.2 Physical Security Incident Reporting

Physical security incidents should be reported directly to UP.

Crime Reports: http://www.northwestern.edu/up/safety/annual-report/csa-crime-report-form.html

8.3 Emergency Mode Operation

Each Student Affairs building has a building manager that is responsible for emergency preparations, fire alarms, automatic sprinklers, emergency lighting, fire extinguishers, etc., coordinated through FM.

8.3.1 Emergency Physical Access

All Northwestern facilities have emergency egress routes posted.

8.3.2 Emergency Data Access

SAIT is reliant on certain university-wide resources, such as the university network and Evanston datacenter, for access to the majority of Student Affairs data. In the event of an emergency, SAIT will work directly with NUIT to provide Student Affairs staff with data access. Where emergency data access does not require NUIT systems, SAIT will work to restore data access.

8.4 Disaster Recovery Planning

A disaster is defined as a major disruption to normal processing due to physical damage to equipment or facilities, or the inability to access or process IT at the facility. An IT Disaster Recovery Plan (DRP) is meant to restore critical IT facilities (data centers, key applications, etc.) and to resume the most critical of services as quickly as possible following a disaster. The Business Continuity portion of a plan provides the subsequent processes and actions required to resume processing in a reduced-capability mode or at alternate sites.

SAIT has established a DRP that includes the following:

- A method for organized assessment of damages to the facilities and equipment
- A means for timely executive decisions to be made regarding restorations
- A plan for establishing temporary operations under likely emergency situations
- A call list for all relevant personnel

NUIT Emergency Management
Operations: http://www.northwestern.edu/up/emergency/overview.html

8.4.1 Applications and Data Criticality Analysis and Ranking

SAIT maintains a ranked list of applications and data resources that represents the order in which facilities will be restored in the event of a disaster. The ranking of each resource is determined by a committee and is a reflection of the necessity of that application to the business operations of Student Affairs as a whole.

8.4.2 Evaluation of Contingency Plans

The SAIT Operations Team meets periodically to review the DRP for currency.

8.4.3 Testing Contingency Plans

Subsets of DRP procedures are tested on rotation to assess the continued technical and logical validity of process.

9.0 Personnel Security

9.1 Hiring

Northwestern University is committed to employing qualified talent and providing a safe environment for all employees and students.

9.1.1 Recruiting and Hiring Procedures

Student Affairs hiring procedures fall under the jurisdiction of Human Resources. Individuals who have been selected as final candidates for staff positions must successfully complete a background check prior to beginning employment in their new positions. Additionally, upon accepting new positions, these individuals must sign an acknowledgement that, where there is reasonable cause to believe that a child known to them in their professional or official capacities may be abused or neglected, they are required to make a report to the Illinois Department of Children & Family Services (DCFS). Human Resources may also require a Non-Disclosure Agreement (NDA), depending upon the position for which an individual is being hired.

Student Affairs staff who come into contact with patient health information (PHI) are also required to sign an NDA. This includes SAIT staff who perform maintenance on systems containing PHI.

Human Resources: http://www.northwestern.edu/hr/

9.1.2 Clearances

The Office of Human Resources utilizes an external vendor to conduct background checks on newly hired and transferring regular staff employees, as well as temporary employees. Background checks, education verification, identity verification, and reference checks are conducted in accordance with applicable privacy and data regulations, and include the following:

- A minimum of two professional references
- Verification of academic degrees received
- Verification of professional certifications when listed as a qualification for the position
- History of any criminal record and registered sexual offender check
- Verification of identity and authorization to work via the federal e-Verify process
- Verification of driving record when operation of a motor vehicle is required for the position

Human Resources Verifications: http://www.northwestern.edu/hr/payroll/e-verify/

9.1.3 Business Associates and Third Parties

Business associates and third parties represent a risk to the university, as they have a different set of motivations and goals than university employees. All business associates should be made aware of and held accountable for all applicable policies and responsibilities of the systems with which they are involved. Contracts with third party vendors must go through NUIT's Project Management Office, which includes a security assessment and contract approval from the Office of General Counsel. SAIT should be included in the vetting process for any third party vendors whose systems handle Student Affairs electronic data. More on shared responsibility for institutional data may be found in the Protocol for Exchange and Shared Responsibility for Institutional Data section above.

9.2 Termination and Transfer

Termination of individuals' access rights to sensitive data and facilities should be completed as soon as feasible and appropriate, especially in the case of non-voluntary terminations. SAIT and the Office of Human Resources should receive notification of terminations made by Student Affairs departments. When staff members are involuntarily terminated for cause, Human Resources will notify ISS/C to immediately disable the staff member's NetID. Revocation of Student Affairs data access privileges is performed by SAIT staff, and may occur more quickly than NetID deauthorization where SAIT has been appropriately advised of change in employment status. For more information on revocation of privileges, see the Revoking Data Access Authorization section above.

9.2.1 Procedure for Exiting Employees

All Student Affairs employees must return any property, materials, and written information issued to them or in their possession on or before the last day of work, including credit cards, ID badges, keys, manuals, calculators, computers, office equipment, key cards, etc. Northwestern will take all appropriate actions to recover or protect its property. To facilitate the termination process and associated system procedures, the Office of Human Resources provides an Employment Termination Checklist that may be used by Student Affairs departments when staff members transfer or exit the organization.

SAIT does not modify or specially monitor data access privileges prior to departure for Student Affairs employees undergoing transfer or other separation under amicable terms unless specifically asked to do so by the relevant department head or Associate Vice President. Where termination is for cause, SAIT should be contacted immediately to remove all data access privileges and tools.

Employment Termination Checklist: http://www.northwestern.edu/hr/policies-forms/policies-procedures/employment/employment_termination_checklist.pdf

9.3 Sanctions

Violations of the Student Affairs security policy will be referred to the appropriate university disciplinary channels and may result in disciplinary action up to and including termination of employment and/or dismissal from the university, in addition to remedies sought by the copyright holder where applicable. Individuals found in violation of policy are subject to consequences as documented in the Staff Handbook, the Standards of Business Conduct, and contractual agreements with third parties.

Staff Responsibilities: http://www.it.northwestern.edu/policies/responsibilities.html
Reporting: http://www.it.northwestern.edu/policies/reporting.html

9.4 Security Training and Awareness

Security threats, attack vectors, and social engineering tactics are constantly evolving. In order to keep Student Affairs mindful of and up-to-date on good security practices, SAIT conducts an ongoing security awareness campaign. This includes display of information security posters at Student Affairs staff locations, distribution of security-related promotional items, and monthly listserv communications with security tips and updates. SAIT also maintains a security page on its website.

10.0 Information Systems Configuration Management

10.1 IT Acquisition, Development, and Deployment

Technological innovations and initiatives within Student Affairs should be brought to SAIT early in their life for consideration and assessment. SAIT will work with end users to review initiatives and determine viability within the Student Affairs IT environment and long-term strategic plan. Before developing, purchasing, or contracting for IT products, vendor services, support, or consultation, SAIT will in turn approach NUIT—or instruct departments to do so—to ensure that all acquisitions, development, and deployments of IT conform to existing Northwestern guidelines to maximize functionality and minimize effort.

All acquisitions and deployments of IT within Northwestern must conform to the guidelines of and be reviewed by NUIT. This includes communication, information storage and processing, and software systems, as well as physical facilities and vendor contracts relating to such systems and services. To submit proposals to NUIT for review or approval, departments must contact the Associate Vice President in the Office of the Vice President for Information Technology; submit a brief description of the project, product, or services; present financial information including anticipated or approved funding sources; and provide vendor product specification documentation and any relevant contracts or agreements. All bid specifications should include a requirement that authentication of users be performed using the NetID and associated password.

IT Guidelines: http://www.it.northwestern.edu/policies/guidelines.html
Acquisition of IT Resources: http://www.it.northwestern.edu/policies/acquisition.html
Purchasing: http://www.northwestern.edu/uservices/purchasing/vendors/ibuynu_marketplace.html

10.2 Configuration Management

All computing equipment—including servers, workstations, mobile devices, printers, faxes, and other devices—owned by Northwestern and issued to Student Affairs employees are logged by SAIT in an inventory tracking system that identifies at minimum the serial number, location, and owner of the equipment. Equipment with inventory tags or costs exceeding $5000 are reported to the Accounting Services Equipment Inventory Coordinator.

Networks

The communications infrastructure of the university is a critical strategic advantage that facilitates teaching, research, and administration. NUIT has established policies to ensure that the university deploys a consistent infrastructure (wired, wireless, video, voice, and converged communications) to Northwestern organizations, programs, or affiliates to minimize costs and maximize the value of these resources. NUIT must review and approve in advance of investigation, purchase, or deployment, any information technology that changes the university's network structure or could compromise the physical or logical security of the network. This includes all hubs, switches, routers, and other equipment that may be connected to the network.

Coordination of Online Services: http://www.it.northwestern.edu/policies/coordinate.html

Infrastructure and Network Facilities: http://www.it.northwestern.edu/policies/infrastructure.html

Servers

Server hardware configurations may vary according to the applications or services hosted, but operating systems, firewalls, backups, and monitoring are built and maintained according to standardized SAIT procedures. Servers hosted in the Northwestern Data Center additionally conform to configuration guidelines provided by the Data Center.

Cloud Computing Services: http://www.it.northwestern.edu/data-centers/nucloud.html

Workstations

SAIT provides a limited number of hardware configuration options for staff desktops and laptops. Department heads must inform SAIT of any Student Affairs staff members with special configuration requirements. Permission for nonstandard configuration may be granted at the discretion of the director of SAIT.

To maintain a consistent level of security and compatibility, all new and repurposed workstations undergo a standard imaging and software configuration process prior to deployment. After distribution, workstation configuration is tracked and occasionally modified using a systems management tool administered by SAIT and licensed centrally by Northwestern. Workstations that may process restricted data are configured as though they will.

Mobile Devices

All mobiles devices, personal or university-owned, that connect to university email accounts have mobile policies enforced by Northwestern's Exchange servers. These policies include a required PIN-lock, remote-wipe capabilities, and other security settings.

10.3 Configuration Change Control

Change management involves the formal introduction and approval of proposed alterations to IT infrastructure and services. The purpose of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes in order to minimize the number and impact of related incidents.

Changes to Student Affairs IT infrastructure and services are discussed and tracked in weekly SAIT meetings, and often involve decision-making or input from other technical experts, managers, or stakeholders. Changes may arise reactively in response to problems, proactively to achieve improvements in efficiency or effectiveness, or as a response to new business initiatives, programs, projects, or service improvements. At a minimum, such changes require the approval of the managers of User Services and Support and the Applications and Infrastructure team.

11.0 Information Systems Security Risk Management

An information systems risk management program is intended to prevent, detect, contain, and correct both deliberate and inadvertent security violations. Using various industry-tested methods of analysis, risks are identified and ranked. Mitigative measures are then identified and subjected to a cost-benefit analysis prior to a final decision on implementation.

Northwestern's information systems risk management program is part of the overarching Northwestern Enterprise Risk Management (ERM) program. Using various analytic efforts, NUIT's Information Systems Security/Compliance (ISS/C) and Audit and Advisory Services (A&AS) teams identify and rank risks for the university as a whole. SAIT's risk management program is informed by ISS/C, A&AS, and industry findings and practices.

Enterprise Risk Management: http://www.northwestern.edu/audit-and-advisory/services/risk-and-control/erm.html

11.1 Risk Identification

Before an effective risk management program can be implemented, environment-specific risks must be identified. As a unit within Northwestern, Student Affairs is exposed to several categories of risk.

Deliberate Attacks

Risk efforts are often focused on attacks that are likely to be initiated in a planned, deliberate manner. The motivation and sophistication of attackers varies, but they generally fall into one of the following categories:

- Disgruntled employees
- Hackers
- Vandals
- Criminals
- Organized Crime
- Nation-states

Northwestern University experiences random malware attacks on an almost daily basis, mitigated by the defensive techniques described in their security policy. Dedicated attacks have been infrequent, with no known major criminal attacks to date. Nevertheless, given the large amount of intellectual, healthcare, and research data contained in university information systems, deliberate attacks are a non-negligible threat for all units within the university, including Student Affairs.

Accidental/Inadvertent Incidents

Information systems are generally designed to minimize the likelihood of unintentional compromise of the system. Security measures must be weighed against system usability, however, meaning that the threat of accidental introduction of vulnerabilities is never zero. Risk management efforts therefore include the identification of potential incidents and the development of policies to mitigate these occurrences, including increasing system user awareness of risks.

Emergencies

Risk management activities also include efforts to determine the types of security incidents and natural phenomena that facilities are likely to experience over their operational lifetime, and how the designs and procedural measures in place would deal with these occurrences. Risk efforts ensure that policies are in place to maintain security while minimizing the damage to or loss of information and information systems in conceivable emergency situations, such as fires, earthquakes, storms, and power surges.

11.2 Risk Analysis/Ranking

Once specific information security risks are identified, an accurate and thorough assessment of their impacts on the confidentiality, availability, and integrity of data must be conducted. This effort provides the information to rank risks in order of likelihood, both of attempt and of success, and consequences. Student Affairs risks are defined and ranked in a format compatible with that used by the Risk Initiative Steering Committee (RISC), which supports the ERM program and efforts conducted by A&AS.

SAIT conducts its risk analysis using risks and consequences identified by ISS/C and A&AS, as well as estimates of likelihood based on national surveys conducted by the Computer Security Institute (CSI) and the Poneman Institute. SAIT also makes use of ISS/C-provided vulnerability assessment services as part of its risk identification and analysis. Security reports or updates prepared and disseminated by ISS/C are reviewed in a timely manner.

Vulnerability Assessment: http://www.it.northwestern.edu/security/vulnerability.html

11.3 Risk Mitigation

Using the risk identifications and ranks gathered during risk analysis, SAIT implements a combination of policy, procedures, and technical measures to mitigate vulnerabilities and risks as resources allow. Risk mitigation measures are developed and implemented by SAIT functional units in conjunction with the director of SAIT and, where applicable, primary stakeholders.

11.4 Risk Reevaluation

Frequent reevaluation of risks is a necessary component of any risk management program. SAIT's risk assessment efforts are performed annually as a self-audit. Periodic audits by A&AS or outside organizations that specialize in risk assessment may be conducted as appropriate.

11.5 Incident Response and Reporting

An IT incident response plan addresses instances in which unauthorized access to or disclosure of information systems/data may have occurred. The plan covers the conditions whereby this process is invoked, the response to such events, the resources required, and the course of recommended action. The primary emphasis of activities described within the incident protocol is the return to a normalized (secure) state as quickly as possible, with a secondary goal of full identification of the events precipitating the incident.

SAIT maintains an Incident Response Team (IRT) to carry out tasks outlined in its incident response plan. This team includes the director of SAIT, as well as key members of the User Services and Infrastructure

teams. For university-wide matters, NUIT has established its own IRT, chaired by the director of ISS/C and composed of members from all relevant Northwestern departments, including Student Affairs.

NUIT Incident Response: http://www.it.northwestern.edu/policies/incident.html

APPENDIX A

SAIT Information Security Policy Traced to ISO, HIPAA, and NUIT Information Security Requirements

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organizations will conduct periodic Risk Analysis efforts. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks.	4.1 Assessing Security Risks	Risk Analysis §164.308(a)(1)	Vulnerability Assessments; Enterprise Risk Management (ERM) group; Threat Assessment Group (TAG) (P)	10.2 IS Risk Analysis/Ranking	10.2 Risk Analysis/Ranking
Organizations will remediate risks identified by the RA activities.	4.2 Treating Security Risks	Risk Management §164.308(a)(1)	Vulnerability Assessments	10.0 Information Systems Risk Management	10.0 Information Systems Risk Management
The organization shall maintain a security policy framework.	5.1 Information Security Policy		NUIT Strategic Plan	NU ISSP/P	SAIT ISSP/P
The organization will maintain a high level security policy that displays management's backing.	5.1.1 High Level Security Policy (HLSP)		NUIT Website	NU ISSP/P	SAIT ISSP/P
The security policy framework is reviewed/evaluated on a periodic basis.	5.1.2 Review and Evaluation		NUIT Security Policies periodic reviews	1.2 Introduction	1.2 Introduction

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization has assigned responsibility for security to an individual or committee.			NUIT Organization	2.0 NUIT Organization	3.0 SAIT Organization
Organizations will maintain current organizational charts	6.1 Internal organization		NUIT Website	2.0 NUIT Organization	3.0 SAIT Organization
Management will show commitment to the security program and its efforts	6.1.1 Management commitment		NUIT Strategic Plan	2.0 NUIT Organization	3.0 SAIT Organization
Measures shall be in place to coordinate information security efforts within groups	6.1.2 Information security coordination		NUIT Management meetings	2.1 NU VP for IT and CIO 7.4 Security Awareness and Training	8.4 Security Training and Awareness
Implement procedures for the authorization and supervision of workforce members who work with sensitive data. Roles should be clearly defined.	6.1.3 Allocation of information security responsibilities	Assigned Security Responsibility §164.308(a)(2)	NUIT IDM Website Data Access Policy	2.0 Northwestern University Information Security Responsibilities	3.0 SAIT Organization 4.2 Data Access Management
Procedures will be in place that require the proper authorization of computing resources before they are allowed in the production environment.	6.1.4 Authorization for facilities		Configuration Management Process	7.1 IT Acquisition, Development and Deployment	9.1 IT Acquisition, Development, and Deployment
The organization will utilize confidentiality agreements to protect its information resources.	6.1.5 Confidentiality agreements		Confidentiality, Non-Disclosure Agreements	3.1 Information Classification	4.1 Information Classification

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
The organization will commit to maintain a relationship with local and federal authorities.	6.1.6 Contact with authorities			3.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data	4.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data
The organization utilizes SME advice for the new projects or major program changes.	6.1.7 Specialist security advice		Consulting Contracts		
Major projects will perform independent review to help reduce risk.	6.1.8 Independent review	Evaluation §164.308(a)(8)	NU ISS/C & Auditing websites	10.4.1 IS Self-Audits and Activity Reviews	11.4 Risk Reevaluation
Maintain security of the organization's information and information processing facilities from external parties	6.2 External parties			6.2 Facility Security Plan	8.1 Facility Security Plan
Organizations will identify risk represented by third-parties	6.2.1 Identification of risks related to external parties		Data Access Policy	10.2 IS Security Risk Analysis/Ranking	11.2 Risk Analysis/Ranking
Organizations will maintain policies for third-party access into the network.	6.2.2 Third party access		NUIT IDM Website Data Access Policy	3.2.3.5 Authentication for Services Outside the University Environment	5.2.3.2 Authentication for Services Outside of the University Environment

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organizations will maintain policies for the outsourcing of resources.	6.2.3 Addressing security in third-party agreements	Business Associate Contracts and Other Arrangement §164.308(b)	Confidentiality, Non-Disclosure Agreements NU Consulting and Project Office website	3.1 Information Classification 3.2.3.5 Authentication for Services Outside the University Environment	5.1 Information Classification 5.2.3.2 Authentication for Services Outside of the University Environment
Organization identifies paper, electronic and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information, except where the comprehensive information security program provides for the handling of all records as if they all contained personal information	7. Asset Management		Use of Computers, Systems, Networks Using Network and Computing Resources	8.2 Configuration Management	10.2 Configuration Management

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization has security policies for employees that take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises. Reasonable restrictions upon physical access to records containing personal information, including a written procedure that sets forth the manner in which physical access to such records is restricted; and storage of such records and data is in locked facilities, storage areas, or containers.	7.1 Responsibility for Assets 7.1.3 Acceptable Use of Assets	Workstation Use §164.310(b)	Appropriate Use of Electronic Resources (pending)	4.0 Acceptable Usage	6.0 Information Systems Acceptable Usage
All information and assets associated with information processing facilities should be owned by a designated part of the organization,	7.1.2 Ownership of Assets	Device and Media Controls §164.310(d)(1)		8.2 Configuration Management	10.2 Configuration Management
Media is labeled so it can be identified by a classification.	7.2 Information Classification		Data Access Policy	8.2 Configuration Management	10.2 Configuration Management
Limit the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected.	11.4.2 Review of User Access Rights			3.1 Information Classification 3.2.1 Access Authorization	5.1 Information Classification 5.2.1 Access Authorization

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Security is clearly defined in job descriptions.	8.1.1 Security roles in job descriptions	Authorization and/or supervision §164.308(a)(3)	NUIT Website Data Access Policy	2.0 Northwestern University Information Security Responsibilities	3.0 SAIT Organization
Organization to determine that the access of a workforce member to specific classifications of electronic information is appropriate.	8.1.2 Personnel screening	Workforce Clearance Procedure §164.308(a)(3)	HR website	3.2.1.1 Eligibility for Information Access	5.2.1.1 Eligibility for Data Access
Organization will clearly review and define terms and conditions.	8.1.3 Terms and conditions				
Organization will monitor traffic leaving the perimeter for violations of policy.	10.6.1 Network Controls 10.10.2 Monitoring System Use		Firewall Policy Privacy Within the NU Network Appropriate Use of Electronic Resources (pending)	5.0 Network Security 5.3 Firewalls 5.11.1 Activity Monitoring 5.11.2 Computer, System, or Network Monitoring	7.0 Network Security 7.4 Firewalls 7.13.1 Activity Monitoring 7.13.2 Computer, System, or Network Monitoring
Organization will review internet activity for appropriate use.	10.10.2 Monitoring System Use		Appropriate Use of Electronic Resources (pending)	5.11.2 Computer, System, or Network Monitoring	7.13.2 Computer, System, or Network Monitoring
Management's responsibilities to technology and security are clearly defined.	8.2.1 Management responsibilities		NUIT Website	2.0 NUIT Organization	3.0 SAIT Organization

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement a security awareness and training program for all members of the organization (including management).	8.2.2 Security awareness	Security Awareness and Training §164.308(a)(5)	NUIT Website	7.4 Security Training and Awareness	9.4 Security Training and Awareness
Implement a disciplinary process for employees that commit a security breech.	8.2.3 Disciplinary Process	Sanction Policy §164.308(a)(1)	HR website NU Staff Handbook	7.3 Sanctions 7.3.1 Security Breaches	9.3 Sanctions
Implement periodic security updates such as quarterly email distribution or poster campaigns.		Security Reminders §164.308(a)(5)	NUIT Website	7.4 Security Training and Awareness	9.4 Security Training and Awareness
Organization has procedures for terminating access to electronic information when the employment of a workforce member ends. Preventing terminated employees from accessing records containing personal information by immediately terminating their physical and electronic access to such records, including deactivating their passwords and user names.	8.3.1 Termination Responsibilities 8.3.2 Return of Assets 8.3.3 Removal of Access Rights	Termination Procedures §164.308(a)(3)(ii)(C)	Employment Termination Checklist NU Staff Handbook	7.2 Terminations and Transfers	9.2 Terminations and Transfers

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information.	9.1.1 Physical security perimeter	Facility Security Plan §164.310(a)	NU Police Department Policies	6.1 Facility Security Plan	8.1 Facility Security Plan
Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. Organization will utilize equipment such as cameras and visitor logs.	9.1.2 Physical entry controls	Access Control and Validation Procedures §164.310(a)	NU Police Department Policies NUDC SOP (Data Center)	6.1.1 Physical Access Controls	8.1.1 Physical Access Controls
Access to the data center, computer room, and sensitive areas of the operations center is controlled through electronic key cards assigned to appropriate employees.	9.1.3 Secure offices, rooms, and facilities		NUDC SOP (Data Center)	6.1.1.1 Entry Control	8.1.1 Physical Access Controls
The data center is equipped to prevent, detect, and suppress environmental factors, such as raised floors, air conditioning, fire and smoke detectors, and fire suppressant systems.	9.1.4 Protecting against external and environment		NUDC SOP (Data Center)	6.1.2 Environmental Controls	8.1.2 Power and Environmental Controls

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a workstation or class of workstation that can access electronic information.	9.1.5 Working in secure areas	Workstation Use §164.310(c)	Appropriate Use of Electronic Resources (pending) NU Police Department Policies NUDC SOP (Data Center)	6.1.1 Physical Access Controls	6.0 Information Systems Acceptable Usage 8.1.1 Physical Access Controls
Organization will have procedures for security loading/delivery areas.	9.1.6 Isolated delivery and loading areas	Facility Security Plan §164.310(a)	NU Police Department Policies NUDC SOP (Data Center)	6.1.1 Facility Security Plan	
Organization will maintain procedures for the proper placements and physical security of technology equipment.	9.2.1 Equipment sitting and protection	Facility Security Plan §164.310(a)	NU Police Department Policies NUDC SOP (Data Center)	6.1.1 Facility Security Plan	8.1 Facility Security Plan
Redundant/fault tolerant power supplies should be utilized where feasible.	9.2.2 Power supplies	Facility Security Plan §164.310(a)	NUDC SOP (Data Center)	6.1.2 Environmental Controls	8.1.2 Power and Environmental Controls
Restrict physical access to publicly accessible network infrastructure (including wireless)	9.2.3 Cabling security	Facility Security Plan §164.310(a)	NUDC SOP (Data Center)	6.1.2 Environmental Controls	8.1.1 Physical Access Controls
Implement policies to maintain and document repairs to physical components.	9.2.4 Equipment maintenance	Maintenance Records §164.310(a)	NUDC SOP (Data Center)	6.1.3 Facility Maintenance Records	8.1.3 Facility Maintenance Records

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Management approves all media that is moved from a secure area (especially when media is distrusted to individuals). Media back-ups will be stored in a secure offsite facility, which may be either an alternate third-party or a commercial storage facility.	9.2.5 Security of equipment off-premises		NUDC SOP (Data Center) Off-Site Data Storage	3.5 Data Backup and Recovery	5.5 Data Backup and Recovery
Policies and procedures to address the final disposition of reuse of electronic hardware or electronic media on which it is stored. Purge, degauss, shred, or otherwise destroy electronic media so that cardholder data cannot be reconstructed.	9.2.6 Secure Disposal/reuse of equipment	Disposal §164.310(d) Media Reuse §164.310(d)	Disposal of Northwestern University Computers	3.6 Data Computing/Media Reuse/ Destruction	5.6 Data Equipment/ Destruction
Organization has procedures for removing technology property when it is no longer in a production capacity.	9.2.7 Removal of property	Device and Media Controls §164.310(d)(1)	System Administration	3.6 Data Computing/Media Reuse/ Destruction	5.6 Data Equipment/ Destruction
Organization will have specific procedures that explain exactly how systems are to be configured and operated. For example, do not use vendor supplied passwords.	10.1.1 Documented operating procedures		Server Security Appropriate Use of Electronic Resources (pending)	4.0 Acceptable Use	6.0 Information Systems Acceptable Use
Change control procedures will be followed for changes in infrastructure.	10.1.2 Change Management		Change Management Process Handbook	8.3 Configuration Change Control	10.3 Configuration Change Control

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Management's control consciousness and organization structure provides for adequately segregated duties within information systems and between information systems and users.	10.1.3 Segregation of duties		System Administration NUDC SOP	4.0 Acceptable Use	6.0 Information Systems Acceptable Use
Development, Staging, Testing, Laboratory and Production environments will be separated by logical or physical means.	10.1.4 Separation of development and operational facilities				
Organization may permit a business associate to create, receive, maintain, or transmit electronic information on the entity's behalf only if the entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.	10.2.1 3rd party service delivery – contract	Business Associate Contracts and Other Arrangement §164.308(b)		3.1 Information Classification 7.1.3 Business Associates and 3rd Parties	5.1 Information Classification 9.1.3 Business Associates and Third Parties
Periodic reports regarding services rendered and any records related to that service that pertains to information security of third parties is conducted.	10.2.2 3rd party monitoring and review	Business Associate Contracts and Other Arrangement §164.308(b)		3.1 Information Classification 7.1.3 Business Associates and 3rd Parties	5.1 Information Classification 9.1.3 Business Associates and Third Parties

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization has policies and procedures for managing the changes involving 3rd parties.	10.2.3 Managing changes to 3rd party services	Business Associate Contracts and Other Arrangement §164.308(b)		7.1.3 Business Associates and 3rd Parties	9.1.3 Business Associates and Third Parties
Organization conducts capacity planning on production systems.	10.3.1 Capacity planning		NUIT Strategic Plan	2.2 NU Information Technology	10.3 Configuration Change Control
A mechanism exists for the acceptance of a system into the environment. Signoff is conducted by the proper management.	10.3.2 System acceptance		System Administration	2.2 NU Information Technology	10.3 Configuration Change Control
Procedures and software exist for guarding against, detecting, and reporting malicious software.	10.4.1 Controls against malicious software	Protection for Malicious Software §164.308(a)(5)	Firewall Policy Guide to Security Web Applications Desktop Security Recommendations	5.5 Malware 4.1 Standard Workstation Configuration 4.1.1 Handling of Compromised Workstations 10.5 IT Security Incident Response and Reporting	7.7 Malware 6.1 Standard Equipment Configuration 11.5 Incident Response and Reporting

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Backup copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.	10.5.1 Information Backup	Device and Media Controls §164.310(d)(1)	Off-Site Data Storage NU security/backup website	3.5 Data Backup and Recovery	5.5 Data Backup and Recovery
Organization has established clear controls around ACLS and firewall type technologies to protect information assets.	10.6.1 Network controls	Integrity Controls §164.312(e)(1)	Firewall Policy Guide to Security Web Applications Desktop Security Recommendations	3.2.1 Access Authorization 5.0 Network Security 5.3 Firewalls	5.2.1 Access Authorization 7.0 Network Security 7.3 Firewalls
Procedures exist for the secure handling of mass media such as tape backups and flash drives.	10.7 Media handling 10.7.1 Management of removal media 10.7.2 Disposal of media	Disposal §164.310(d) Media Reuse §164.310(d) Device and Media Controls §164.310(d)(1)	Off-Site Data Storage Appropriate Use of Electronic Resources (pending)	3.5 Data Backup and Recovery 3.5.3 Portable Memory Devices 3.5.5 Enterprise Storage Systems and Tape Libraries Backup	5.5 Data Backup and Recovery 6.1 Standard Equipment Configuration 5.6 Data/Equipment Destruction

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization has policies and procedures for the exchanging of data with external parties.	10.8.1 Exchange of info and software		Protocol for Exchange and Shared Responsibility for Institutional Data	3.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data	5.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data
Media will be sent via secure courier or a delivery mechanism that can be accurately tracked.	10.8.3 Physical media in transit		Off-Site Data Storage	3.5 Data Backup and Recovery	5.5 Data Backup and Recovery
Sensitive communications conducted over email is secured by a form of encryption.	10.8.4 Electronic messaging	Method to Authenticate Electronic PHI §164.312(c)(1)	Data Encryption	3.3.3 Securing Communications	7.9 Transmission Security
Implement security measures to ensure that electronically transmitted information is not improperly modified without detection.	10.9.1 Electronic commerce security	Integrity Controls §164.312(e)	Data Encryption	3.3.3 Securing Communications	7.9 Transmission Security 5.4 Data Integrity
Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	10.9.2 On-line transactions	Integrity Controls §164.312(e)	Data Encryption	3.3.2 Securing Data – Data Encryption 3.3.3 Securing Communications 3.4 Data Integrity	5.3.2 Data Encryption 7.9 Transmission Security 5.4 Data Integrity

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Publically available systems are protected to ensure sensitive information is protected.	10.9.3 Publicly available systems		Appropriate Use of Electronic Resources (pending) Server Security	4.1 Standard Workstation Configuration 10.1.1 Deliberate Attacks	6.1 Standard Equipment Configuration 11.1 Risk Identification
Policies and procedures exist to create and maintain retrievable exact copies of electronic assets.	10.5 Backup	Data Backup Plan §164.308(a)(7) Data Backup and Storage §164.310(d)	Off-Site Data Storage NUDC SOP (Data Center)	3.5 Data Backup and Recovery	5.5 Data Backup and Recovery
Procedures are established for the use of information processing facilities.	11.1 Business Requirement for Access Control 9.1.3 Securing offices, rooms, and facilities	Information Security Activity Review §164.308(a)(1)	NUDC SOP (Data Center)	6.1 Facility Security Plan	8.1 Facility Security Plan

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement technical policies and procedures for electronic information systems that maintain information to allow access only to those persons or software programs that have been granted access rights as specified. Limit access to those persons who are reasonably required to know such information in order to accomplish such purpose or to comply with state or federal record retention requirements.	11.1.1 Access control policy	Information Access Management §164.308(a)(4)	Data Access NetID and Network Privileges	3.2 Data Access Management	5.2 Data Access Management
Limit access to computing resources to only those individuals whose job requires such access.	11.2 User access management	Information Access Management §164.308(a)(4)		3.2.1.3 Changing Information Access Authorizations	5.2.1.3 Changing Data Access Authorizations
Organization has policies and procedures for granting access to electronic assets. For example, through access to a workstation, transaction, program, process, or other mechanism (requests, identify the role, approvals, statement of rights, unique ID).	11.2.1 User registration	Access Authorization §164.308(a)(4) Unique User Identification §164.312(a)	Net ID and Password Security	3.2.1.1 Eligibility for Information Access 3.2.3 Workforce Member Authentication	5.2.1.1 Eligibility for Data Access 5.2.3 Workforce Member Authentication

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement policies and procedures for granting access to electronic assets. For example, through access to a workstation, transaction, program, process, or other mechanism. Ensure proper user authentication and password management for non-consumer users and administrators, on all system components.	11.2.2 Privilege management	Access Authorization §164.308(a)(4)	Net ID and Password Security	3.2.3 Workforce Member Authentication	5.2.3 Workforce Member Authentication
Organization has procedures for creating, changing, and safeguarding passwords. Access to user identification is blocked after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system.	11.2.3 Password management	Password Management §164.308(a)(5)	Password/Passphrase Net ID and Password Security	3.2.3.1 Password Construction Requirements 3.2.3.2 Password Management	5.2.3.3 Password Construction Requirements 5.2.3.2 Password Management
Organization has policies and procedures that review, and modify a user's right of access to a workstation, transaction, program, or process. Restricting access to active users and active user account only.	11.2.4 Review of rights	Access Establishment and Modification §164.308(a)(4)		3.2.1.3 Changing Information Access Authorizations	5.2.1.3 Changing Data Access Authorizations
User responsibilities are clearly documented and signed off by the user in an employee agreement.	11.3 User responsibilities		Network User Access Form	3.2.1.1 Eligibility for Information Access	5.2.1.1 Eligibility for Data Access

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Maintain a record of the movements of hardware and electronic media and any person responsible therefore.		Accountability §164.310(d)		8.2.4 Workstations Configuration Management	10.2 Configuration Management
Policies and procedures exist for the correct use and management of passwords.	11.3.1 Password usage	Password Management §164.308(a)(5)	Password/Passphrase	3.2.3.2 Password Management	5.2.3.2 Password Management
Unattended equipment will be secured by timeouts, locking screens, logoffs, etc.	11.3.2 Unattended equipment	Workstation Security §164.310(c)		5.4.1 Logging-in	7.5 Workstation and Network Access
Organizations will implement a clean desk policy to protect physical assets such as electronics and paper.	11.3.3 Clear desk policy				
Clear policies exist detailing the use of network services and restrictions.	11.4.1 Policy on use of network services		Using Network and Computing Resources	5.2 Network User Rights and Responsibilities	7.2 Network User Rights 7.3 Network User Responsibilities
Authentication will be required for any access across external or public networks.	11.4.2 User authentication for external connections	Person or Entity Authentication §164.312(d)	Using Network and Computing Resources	3.2.3.3 NU Network Authentication	7.5 Workstation and Network Access 7.10 Remote Access 7.11 Wireless Access

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Workstations will be authenticated before they are allowed to access network resources.	11.4.3 Node authentication		Data Access Software Authentication Requirements	5.8 Remote Access 5.12 Software Authentication	7.5 Workstation and Network Access 7.10 Remote Access
Organization will implement security for the protection of side band or diagnostic ports in equipment.	11.4.4 Remote diagnostic port protection				
Networks will be segmented where logically applicable. Segmentation will serve to protect information assets.	11.4.5 Segregation in networks				
Processes are in place to control access to what is placed on the internal or external network.	11.4.6 Network connection control				7.5 Workstation and Network Access
Static and dynamic routing protocols will be managed by the appropriate individuals and with security as a priority.	11.4.7 Network routing control				
Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation.	11.5 Operating system access control	Workstation Use §164.310(b)	Appropriate Use of Electronic Resources (pending) Security Recommendations for Desktop Computers	4.1 Standard Workstation Configuration	6.1 Standard Equipment Configuration

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Use windows to restrict access to resources based on user or computer logon procedures, identification, password management, utilities, timeout, and connection time. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	11.5.1 Terminal log-on procedures	Person or Entity Authentication §164.312(d)	Net ID and Password Security	3.2.3.3 NU Network Authentication	7.5 Workstation and Network Access
Users will be authenticated using industry standards, recommended practices method to ensure the account being utilized is the correct individual.	11.5.2 User identification and authentication	Access Controls §164.312(a)(1) c Person or Entity Authentication §164.312(d)	Net ID and Password Security	3.2.3 Workforce Member Authentication	5.2.3 Workforce Member Authentication
Organization will provide procedures for the management of passwords, recovery and resets.	11.5.3 Password management system	Password Management §164.308(a)(5)	IDM Website	3.2.3.2 Password Management	5.2.3.4 Password Management
System utilities will only be used if authorized and needed for the job. Utilities such as password crackers are forbidden.	11.5.4 Use of system utilities				
Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	11.5.5 Session timeout	Automatic Logoff §164.312(a)	Using Network and Computing Resources	5.4.1.3 Inactivity Log-off	7.5.3 Inactivity

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Implement electronic procedures that terminate a network session after a predetermined time of inactivity.	11.5.6 Limitation of connection time			5.4.1.3 Inactivity Log-off	7.5.3 Inactivity
Applications define controls around information accessed inside the application.	11.6.1 Information access restriction	Access Establishment and Modification §164.308(a)(4)			5.2.3.1 Software Applications Authentication
Data will be isolated, depending on its purpose, for sensitivity. De-identification is preferred.	11.6.2 Sensitive system isolation				
Implement procedures to regularly review records of information security activity, such as audit logs, access reports, and security incident tracking reports. Including: FW, individual user accesses to cardholder data, actions taken by any individual with root or administrative privileges, creation and deletion of system-level objects, date and time, etc. Review logs for all system components at least daily. Log reviews should include those servers that perform security functions like Intrusion Detection System (IDS) and Authentication, Authorization, and Accounting (AAA) servers (for example, RADIUS)	10.10.1 Audit logging 10.10.2 Event logging	Information System Activity Review §164.308(a)(1) Audit Controls §164.312(b)		5.11.2 Computer, System, or Network Monitoring	7.13.1 Activity Monitoring

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Procedures for monitoring log-in attempts and reporting discrepancies.	10.10.2 Event logging 10.10.5 Fault logging	Log-in Monitoring §164.308(a)(5)		5.11.3 Data Search Utilities	6.1 Server Configuration
Synchronize all critical system clocks and times	10.10.6 Clock synchronization			5.4.2 Network Time Protocol	7.6 Network Time Protocol
Policies and procedures exist for the correct use of mobile computing devices such as laptops and smart phones. The mobile devices will be protected using encryption, authentication, templates, timeouts, etc.	11.7.1 Mobile computing		Mobile Device Security Guidelines	4.4 Mobile Devices	6.1 Standard Equipment Configuration
Policies and procedures exist for the correct use of tele-working.	11.7.2 Tele-working		Usage of the NU SSL VPN	5.3.8 Usage of the NU SSL VPN	7.10 Remote Access
Develop applications based on secure coding guidelines and business requirements.	12.1 Security requirements of information systems				7.12 Secure Web Applications and Coding
Implement electronic mechanisms to corroborate that electronic data has not been altered or destroyed in an unauthorized manner	12.2 Correct processing in applications	Mechanism to Authenticate Electronic PHI §164.312(c)	Data Encryption	3.4 Data Integrity	5.4 Data Integrity

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Application will validate data being submitted to the system to check for validity.	12.2.1 Input data validation			3.4 Data Integrity	5.4 Data Integrity 7.12 Secure Web Applications and Coding
Organization will have policies and procedures to ensure the internal processing of applications is correct.	12.2.2 Control of internal processing	Integrity Controls §164.312(c)(1)			
Applications utilizing data exchange will use message authentication to maintain integrity.	12.2.3 Message integrity		Protocol for Exchange and Shared Responsibility for Institutional Data	3.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data	5.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data
Applications will validate the data being presented as output to ensure the data is correct.	12.2.4 Output data validation				
Implement a method to encrypt and decrypt sensitive data and manage encryption keys securely. Data on laptops and portable systems will utilize encryption to protect data at rest.	12.3 Cryptographic controls	Encryption and Decryption §164.312(a) Encryption §164.312(e)(1)	Data Encryption	3.3.2 Data Encryption	5.3.2 Data Encryption
Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.	12.4 Security of system files				

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization has policies for securing operating systems that applications run on. (hardening guides, templates, base images, peer review)	12.4.1 Control of operational software				6.1 Standard Equipment Configuration
Separation of duties between development/test and production environments.	12.4.2 Protection of system test data	Access Control and Validation Procedures §164.310(a)			
Organization controls access to source code and log files. Provide centralized servers or media that is requires authorization and is difficult to later manipulate.	12.4.3. Access control to source code and logs	Access Control and Validation Procedures §164.310(a)			
Organization has policies and procedures to detect and remedy information leakage from applications.	12.5.4 Information leakage				
Policies and procedures exist for the outsourcing of development efforts. These policies detail how the code will be secured, reviewed, and owned.	12.5.5 Outsourced development management				

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organization will perform vulnerability management. Review custom application code to identify coding vulnerabilities. Cover prevention of common coding vulnerabilities in software development processes. Deploy IDS to monitor traffic.	12.6 Vulnerability management		Vulnerability Management Program website	5.10.1 Web Assessments 10.2 IS Security Risk Analysis/Ranking	7.12 Secure Web Applications and Coding 11.2 Risk Analysis/Ranking
Organization has a comprehensive change management policy and detailed procedures.	12.5 Security in development and support		Change Management Process	8.3 Configuration Change Control	10.3 Configuration Change Control
Each change request is entered into a CMDB, which is used to coordinate the change process, authorization and track the status of outstanding change requests.	12.5.1 Change control		Change Management Process	8.3.1 Change Approval Board	
Perform testing in response to environmental or operational changes.	12.5.2 Technical review following a change	Evaluation §164.308(a)(8)		6.4.3 Testing Contingency Plans	8.4.3 Testing Contingency Plans
Organization has controls around the ability to modify code or deploy executables into the production environment.	12.5.3 Restrictions on change			8.3 Configuration Change Control	
Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	13.1 Responding to incidents	Response and Reporting §164.308(a)(6)	Incident Response Protocol	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.	13.1.1 Reporting security incidents	Response and Reporting §164.308(a)(6)	Incident Response Protocol Reporting a Violation	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting
Response teams have follow up meetings to discuss weaknesses found during incident investigations.	13.1.2 Reporting weaknesses		Incident Response Protocol	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting
Incident response teams report to management when malfunctions are discovered.	13.2 Reporting software malfunctions		Incident Response Protocol	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting
Policies and procedures exist for dealing with incidents.	13.2.1 Incident management procedures		Incident Response Protocol	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting
Meetings are scheduled for post incident response. These meetings allow teams to learn from the incident.	13.2.2 Learning from incidents		Incident Response Protocol	10.5 IT Security Incident Response and Reporting	11.5 Incident Response and Reporting
Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	14.1.1 Include information security in the business continuity management process	Application and Data Criticality Analysis §164.308(a)(7) Contingency Operations §164.310(a)	NUIT DRP	6.4 Disaster Recovery Planning 6.4.1 Applications and Data Criticality Analysis	8.4 Disaster Recovery Planning 8.3 Emergency Mode Operation

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Organizations will conduct a BIA with regard to the importance of assets and what they are worth.	14.1.2 Business impact analysis	Application and Data Criticality Analysis §164.308(a)(7)	NUIT DRP	6.4.1 Applications and Data Criticality Analysis	8.4.1 Applications and Data Criticality Analysis
Establish (and implement as needed) procedures to restore any loss of data.	14.1.3 Writing and implementation plan	Disaster Recovery Plan §164.308(a)(7)	NUIT DRP	6.4 Disaster Recovery Planning	8.4 Disaster Recovery Planning
Establish procedures to enable continuation of critical business processes for protection of the security of electronic assets.	14.1.4 Planning framework	Emergency Mode Operation Plan §164.308(a)(7) Contingency Operations §164.310(a)	NUIT DRP	6.4 Disaster Recovery Planning	8.4 Disaster Recovery Planning
Procedures for periodic testing and revision of contingency plans. Backup tapes should be restored to ensure they contain valid data.	14.1.5 Testing and maintaining	Testing and Revision Procedure §164.308(a)(7) Emergency Access Procedure §164.312(a)	NUIT DRP	6.4.2 Evaluation of Contingency Plans	8.4.2 Evaluation of Contingency Plans

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P	SAIT ISSP/P
Compliance with Legal Requirements, Security policies, auditing controls	15.1 Compliance with legal requirements 15.2 Compliance with Security policies 15.3 Information systems audits	Evaluation §164.308(a)(8)	NU General Counsel website Vulnerability Management Program website NU Auditing website	12.0 Applicable Requirements 10.2 IS Security Risk Analysis/Ranking 10.4.1 IS Self-Audits and Activity Reviews	4.0 Applicable Requirements 11.2 Risk Analysis/Ranking