

**Northwestern University Information Technology
Information Systems Security Plan/Practices**

**Prepared by:
Ronald Gault Consulting, LLC and
NUIT Information and Systems Security/Compliance**

**August 08, 2014
Version 1.2**

TABLE OF CONTENTS

1.0 INTRODUCTION.....	1
1.1 Purpose	1
1.2 Scope.....	1
2.0 NORTHWESTERN UNIVERSITY INFORMATION SECURITY RESPONSIBILITIES	2
2.1 Northwestern University Vice-President for Information Technology and Chief Information Officer (CIO) and Associate Vice-President and Deputy CIO	2
2.2 NU Information Technology (NUIT)	2
2.2.1 Information and Systems Security/Compliance (ISS/C)	2
2.2.2 Telecommunications and Network Services (TNS)	2
2.2.3 Cyber Infrastructure (CI).....	2
2.2.4 Technology Support Services (TSS)	3
2.3 Other Departmental IT Groups	3
2.4 Offices of General Counsel, Human Resources, Auditing and Advisory Services	3
3.0 PROTECTION OF NU INFORMATION	4
3.1 Information Classification	4
3.2 Data Access Control/Management.....	4
3.2.1 Access Authorization.....	5
3.2.2 Workforce Member Identification	6
3.2.3 Workforce Member Authentication - Passwords.....	6
3.3 Confidentiality/Privacy	7
3.3.1 Secure Handling of Social Security Numbers	8
3.3.2 Securing Data - Data Encryption.....	8
3.3.3 Securing Communications	8
3.4 Data Integrity	9
3.5 Data Backup and Recovery.....	9
3.5.1 Workstations (desktops, laptops) Backup.....	9
3.5.2 Portable Memory Devices Backup	9
3.5.3 Server Backup.....	10
3.5.4 Enterprise Storage Systems & Tape Libraries Backup.....	10
3.6 Data Computing/Media Reuse/Destruction	10

3.6.1	Data Media Destruction.....	10
3.6.2	Software Reuse/Destruction	11
3.6.3	Paper Destruction.....	11
4.0	ACCEPTABLE USAGE	12
4.1	Standard Workstation Configuration.....	12
4.1.1	Handling of Compromised Workstations.....	12
4.2	Laptops	12
4.3	Personal Computers.....	12
4.4	Mobile Devices	12
4.5	Servers	13
4.6	Software.....	13
4.7	Printers, Scanners, Copiers, and Faxes.....	13
4.8	Email.....	14
5.0	NETWORK SECURITY	15
5.1	Network Service Eligibility	15
5.2	Network User Rights and Responsibilities	15
5.3	Firewalls.....	15
5.4	Computer and Network Security Requirements	15
5.4.1	Logging-in.....	16
5.4.2	Network Time Protocol.....	16
5.5	Malware	16
5.5.1	Anti-Virus.....	16
5.6	Server Security	17
5.7	Transmission Security	17
5.8	Remote Access.....	17
5.8.1	VPN	17
5.8.2	SSL VPN (Secure Sockets Layer Virtual Private Network).....	18
5.9	Wireless Access	18
5.10	Secure Web Applications and Coding.....	18
5.10.1	Web Assessments	18

5.11	Accountability.....	19
5.11.1	Activity Monitoring.....	19
5.11.2	Computer, System, or Network Monitoring.....	19
5.11.3	Data Search Utilities	19
6.0	PHYSICAL SECURITY	20
6.1	Facility Security Plan	20
6.1.1	Physical Access Controls.....	20
6.1.2	Environmental Controls.....	20
6.1.3	Facility Maintenance Records	20
6.2	Physical Security and Incident Reporting	20
6.2.1	Incident Handling/Responding	21
6.3	Emergency Mode Operation.....	21
6.3.1	Emergency Physical Access Control	21
6.3.2	Emergency Access to Data.....	21
6.4	Disaster Recovery/Business Continuity Planning	21
6.4.1	Applications and Data Criticality Analysis and Ranking.....	22
6.4.2	Evaluation of Contingency Plans	22
6.4.3	Testing Contingency Plans	22
7.0	PERSONNEL SECURITY AND HUMAN RESOURCES	23
7.1	Hiring	23
7.1.1	Recruiting and Hiring Procedures	23
7.1.2	Clearances	23
7.1.3	Business Associates and 3 rd Parties.....	23
7.2	Terminations and Transfers.....	24
7.2.1	Procedure for Exiting Employees.....	24
7.3	Sanctions	24
7.3.1	Security Breaches	25
7.4	Security Training and Awareness.....	25
7.4.1	New Hire.....	25
7.4.2	Recurrent Training.....	26

8.0	INFORMATION SYSTEMS CONFIGURATION MANAGEMENT	27
8.1	Information Technology Acquisition, Development and Deployment	27
8.2	Configuration Management	27
8.2.1	Networks	28
8.2.2	Servers Configuration Management	28
8.2.3	Software Configuration Management	28
8.2.4	Workstations Configuration Management	29
8.2.5	Portable Devices Configuration Management	29
8.2.6	Devices and Media Accountability	29
8.3	Configuration Change Control	29
8.3.1	Change Approval Board (CAB)	29
9.0	PAYMENT CARD DATA PROTECTION	31
9.1	eCommerce Operations	31
9.2	Annual Self-Assessment Questionnaires	31
9.3	Conducting SAQs	31
9.4	PCI Firewalls	31
10.0	INFORMATION SYSTEMS (IS) SECURITY RISK MANAGEMENT	32
10.1	IS Security Risk Identification	32
10.1.1	Deliberate Attacks	32
10.1.2	Accidental/Inadvertent Incidents	32
10.1.3	Emergencies	32
10.2	IS Security Risk Analysis/Ranking	32
10.2.1	Information Systems Activity Reviews	33
10.3	IS Security Risk Mitigation	33
10.4	IS Risk Reevaluation	33
10.4.1	IS Self-Audits and Activity Reviews	33
10.4.2	IS External Audits	33
10.5	IT Security Incident Response and Reporting	33
10.5.1	IT Incident Response Team	33
11.0	DEFINITIONS	34

12.0 APPLICABLE REQUIREMENTS.....	36
12.1 NU Information Technology, Technology-Related Policies	36
12.2 Health Insurance Portability and Accountability Act (HIPAA) Security Rules and the HITECH Act	36
12.3 National Institute of Standards (NIST) – guidance only	36
12.4 Federal Information Security Management Act (FISMA).....	36
12.5 Family Education Rights and Privacy Act (FERPA)	36
12.6 ISO Information Security Standards	36
12.7 Illinois Personal Information Protection Act (PIPA), 815 ILCS 530/1	36
12.8 Gramm-Leach-Bliley Act (GLBA).....	36
12.9 Payment Card Industry (PCI) Data Security Standard (DSS)	36

**Appendix One - NUIT Information Security Policy Traced to ISO and HIPAA
Information Security Requirements**

Revision Data

Date	Version	Comments	Modified by
15 Nov 2013	1.0	Publish	D. Kovarik
19 Nov 2013	1.1	Correction of minor errors	D. Kovarik
08 Aug 2014	1.2	Minor corrections and additions	D. Kovarik

1.0 INTRODUCTION

The Northwestern University (NU) Information Technology (NUIT) and other NU policies institute an operational and secure information framework that provides the NU community with expeditious access to accurate data, the procedures for appropriate use of that data, and helps to ensure a high level of confidentiality for that data.


1.1 Purpose

This document summarizes the Information Technology policies and procedures that NU has enacted to communicate to the University community an overall understanding of the NU information security architecture and how to operate within it. Specific details are found in the links to policies, procedures, websites, forms, etc. included herein. Information Security ultimately relies on the people involved with the systems; in service of this position, this document is aimed at ensuring the broadest understanding for the broadest audience.

1.2 Scope

The policies summarized herein cover all facilities under the auspices of NUIT. Definitive and documented policies improve the ability of the organization to properly manage access to its data in compliance with applicable Federal and State laws and regulations, and other NU requirements. Anyone observing a violation of the policies mentioned herein must promptly notify their management and any of the following:

- NUIT - [NUIT Support Center](#), (847) 491-HELP (1-4357)
- NUIT – CyberInfrastructure Service Operations: (847) 467-6662 (7-6662)
- E-mail: security@northwestern.edu
- Ethics and Compliance
 - Hotline: (866) 294-3545 or Web site
 - Web site: www.northwestern.edu/ethics

Any request for an exception to NUIT policies should be submitted to NUIT Information Systems Security/Compliance (ISS/C) using the form described in [Exception Request - Appendix A](#) 

ISS/C will coordinate requests for exception to this policy and contact the respective policy owner, data steward and other authorities as deemed appropriate for consideration and discussion of the exception request. Request forms must be completed fully; incomplete forms will be returned without processing. Requestors will be provided with a decision within ten (10) working days from receipt of the completed request.

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

2.0 NORTHWESTERN UNIVERSITY INFORMATION SECURITY RESPONSIBILITIES

NU information security responsibilities are distributed amongst the following offices:

2.1 Northwestern University Vice-President for Information Technology and Chief Information Officer (CIO) and Associate Vice-President and Deputy CIO

The CIO's office provides leadership for the continued development of an innovative, robust, and secure information technology environment throughout the university. The primary responsibility is the development and use of information technology in support of Northwestern's vision for excellence in research, life-long learning, and the administration of the University.

See: <http://www.northwestern.edu/ovp-information-technology/>

2.2 NU Information Technology (NUIT)

Northwestern's information technology organization, NUIT is committed to listening to and collaborating with our business partners, and leading the delivery of the technology services and information resources within the dynamic environment of Northwestern University.

NUIT Organization: <http://www.it.northwestern.edu/about/organization/index.html>

NUIT Structure: <http://www.it.northwestern.edu/bin/docs/NUITOrganization.pdf>

2.2.1 Information and Systems Security/Compliance (ISS/C)

Enables the University to conduct its business in a secure manner while achieving regulatory compliance and providing the controlled sharing of data. It has responsibility for information security, security awareness and training, selection of INFOSEC products; also responsible for generating and implementing the information security policies and procedures to prevent, detect, contain, and correct security violations.

ISS/C: <http://www.it.northwestern.edu/about/departments/issc/index.html>

2.2.2 Telecommunications and Network Services (TNS)

Plans, operates, and maintains the University's transmission networks for voice, data, cellular, wireless, and video services along with all connections to regional and national networks. Communication-oriented applications on the network for voice, voice mail, IP-services, security, etc. are also operated by TNS. Has responsibility for implementing and maintaining information communications networks, including the very important Internet links between the University community and the outside world.

Cyberinfrastructure: <http://www.it.northwestern.edu/about/departments/cyb/index.html>

2.2.3 Cyber Infrastructure (CI)

Provides and supports an infrastructure that meets the needs of the University's teaching, research, and administrative community. Has overall responsibility for the day-to-day operation of the NU data centers.

Cyberinfrastructure: <http://www.it.northwestern.edu/about/departments/cyb/index.html>

2.2.4 Technology Support Services (TSS)

Assists Northwestern faculty, staff, and students in the use of computing and network resources available on campus and over the Internet; educates and informs the University community about new and changing technology at Northwestern, and provides support services to schools and departments. TSS is also the customer service organization for telecommunications services provided by NUIT.

TSS: <http://www.it.northwestern.edu/about/departments/tss/index.html>

2.3 Other Departmental IT Groups

Individual business units are ultimately responsible for the development, documentation and implementation of applicable procedures and equipment to implement and support University policies; procedures are subject to review by ISS/C and/or Audit and Advisory Services (A&AS). Most maintain an internal IT support staff that coordinates activities through the identified NUIT offices.

2.4 Offices of General Counsel, Human Resources, Auditing and Advisory Services

Provide guidance on the implementation of regulatory and program requirements (e.g., HIPAA/HITECH, FERPA, etc.), personnel policies, performance of risk assessments, etc.

See: **General Counsel**

<http://www.northwestern.edu/general-counsel/practice-areas/index.html>)

Human Resources (<http://www.northwestern.edu/hr/>)

Audit and Advisory Services (<http://www.northwestern.edu/audit-and-advisory/>)

3.0 PROTECTION OF NU INFORMATION

NU information is one of its greatest assets and must be consistently protected throughout its life cycle, or to a time when its value or sensitivity is no longer relevant, in a manner commensurate with its sensitivity and criticality, regardless of where it resides or what purpose(s) it serves.

3.1 Information Classification

Classifying information provides a means whereby the level of protection afforded can be matched to the sensitivity and value of that data. Classifying data is a collaborative process requiring the active participation of data owners who have the greatest familiarity with the data, and who are indispensable in accurately identifying the value and sensitivity of individual and aggregated data items.

NU has identified three categories within its data classification scheme:

PUBLIC Information: Information that is available to all members of the NU community, and may be released to the general public.

INTERNAL Information: Information that is intended for use by and made available to members of the NU community who have a business need to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use. Internal information is not intended for public dissemination but may be released to external parties to the extent there is a legitimate business need.

LEGALLY/CONTRACTUALLY RESTRICTED Information: Information that requires protection by applicable law or statute (e.g., HIPAA/HITECH, FERPA, the Illinois Personal Information Protection Act, non-disclosure agreement, contract terms, etc.) or if disclosed to the public could expose NU to undesirable legal or financial obligations.

Data Access Classification: <http://www.it.northwestern.edu/policies/dataaccess.html>

Sensitive Data in Contracts:

<http://www.it.northwestern.edu/policies/contractlanguage.html>

Service Provider Security Assessment:

<http://www.it.northwestern.edu/about/departments/itms/cpo/assessment.html>

3.2 Data Access Control/Management

NU is committed to nurturing the open, information-sharing requirements of its academic culture, while preserving the confidentiality, integrity and availability of its information resources. Access to data will be as broad as possible, consistent with the classification of the data, role(s) and responsibilities of the user, and level of training.

3.2.1 Access Authorization

A wide group of systems, business units, and individuals require data access and therefore must share responsibility for use of that data. As part of this shared responsibility and in the process of managing their data, individual business units are responsible for following the NU policies in the development and implementation of procedures to protect and control access to their data.

3.2.1.1 Eligibility and Authorization for Information Access

The University offers network privileges for scholarship and university business purposes only. Eligibility is typically extended to individuals within these categories: full/part time students, faculty, full/part time staff, retired faculty and staff, temporary and contract employees, visitors, and approved organizations and affiliates. When the responsible supervisor determines accesses required, a request for access is submitted to NUIT who upon approval, will issue an unique network user identification (NetID) to the individual.

NetID and Network Privileges: <http://www.it.northwestern.edu/policies/acctprivs.html>

Non-disclosure Agreements Guide: <http://www.it.northwestern.edu/policies/nda.html>

3.2.1.2 Short-term Authorization

NetIDs can be provided and administered by departments or NUIT, permitting short-term visitors with limited access to the University network and/or resources. These short-term visitors can include vendors demonstrating products/services, seminar or conference attendees, visiting scholars, etc.

NetID and Network Privileges: <http://www.it.northwestern.edu/policies/acctprivs.html>

3.2.1.3 Changing Information Access Authorizations

A transfer to a different department, assumption of new/different duties, new systems, etc. often require a change in an individuals access to University resources. In these instances, NUIT recommends: a) removing access to the specific University services that are no longer part of the job responsibility as soon as the change transpires, and b) requesting access to the resources required of the new position or duties.

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

3.2.1.4 Revoking Information Access Authorizations

All NetIDs are subject to an automatic expiration process, driven primarily by the authoritative systems (e.g., Human Resources, Student Enterprise System, etc.). Transfers, reassignment of duties, retirement and separation from University service typically call for or result in revocation of access, and most often with some sense of immediacy. It is advisable that revocations be specifically requested where access is no longer required, with the auto-expiration viewed as a safeguard. For cases of involuntary termination, immediate revocation is essential. Further, NetID deactivation only removes access to systems that are NetID authenticated, so additional steps may be required to ensure revocation of access.

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

3.2.1.5 Protocol for Exchange and Shared Responsibility for Institutional Data

There are many occasions where data is shared between enterprise application systems and Local Management Information Systems (LMIS). In these cases, it is important to document the data-sharing instance and to capture the mutual agreement to share data, the data elements to be shared, under what conditions the data is to be provisioned, and define the responsibilities and security needs associated with the data provisioning.

[Protocol for Exchange and Shared Responsibility for Institutional Data](#) 

3.2.2 Workforce Member Identification

An authorized user of University resources is assigned a unique identifier, known as the NetID; NetIDs are never reassigned or reused. The most common sources for a NetID are the Human Resources and Student Enterprise systems. Under certain circumstances, a NetID can be created through a manual process. The most common format of a NetID is a combination of three letters and three numbers and should not be confused with seven-digit student/employee number.

The NetID is most commonly used to access these University systems:

- University e-mail
- NU online directory
- NU Library online resources
- Grades and transcripts (CAESAR)
- Kronos Time System
- Campus wireless network
- Off-campus access to the NU Network (VPN)

Based on your University affiliation (faculty, staff, student, or a combination of staff/student, etc.), the NetID provides you with role-specific access to University systems. **NetID:** <http://www.it.northwestern.edu/netid/overview.html>

3.2.3 Workforce Member Authentication - Passwords

Authentication of users is performed using the NetID and its 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. NUIT makes available several authentication methods for use by information systems and applications, e.g., Web Single Signon (SSO), Microsoft's Active Directory, Lightweight Directory Access Protocol (LDAP), federated authentication, etc. The user attributes and group membership data contained within the authentication systems is classified "Legally/Contractually Restricted"; any access of this data must be requested of and approved by the administrative unit that is providing the data. **Identity Services:**

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

3.2.3.1 Password Construction Requirements

Your NetID password, in conjunction with your NetID, is used to validate your identity on the NU Network. As your key to the network, University systems and resources, and your personal account information, your password should be guarded carefully and never shared with anyone; it is a violation of University policy to share your password. Though you may be prompted to provide your password at a signon page, any other solicitation of your password is a violation of University policy. For a complete description of how to select a secure **Password**, e.g., minimum/maximum length, allowable characters, etc.: <http://www.it.northwestern.edu/netid/password.html>

3.2.3.2 Password Management

As a password ‘ages’, its risk of being compromised increases. NU uses a password aging system that requires you to periodically change your NetID password. You will receive several e-mail reminders to change your password as the expiration date approaches. You may change your password more frequently than what is required, but you must change it at least once during the defined period. If you have forgotten your password, or let your password expire, contact your NetID administrator or go to:

Restoring Your Password: <http://www.it.northwestern.edu/netid/resetguidelines.html>

3.2.3.3 Software Applications Authentication

For added security, some software applications may require additional information about the user for authorization decisions. The University makes available several authentication methods for use by software applications beside those that may be built into the application. If a Web-based application cannot be modified to conform NetID-based access control, then it should be implemented by use of the Web SSO system (Online Passport), which will authenticate the user before passing control to the application.

User Authentication Services: <http://www.it.northwestern.edu/auth-svcs/index.html>

Software Authentication: <http://www.it.northwestern.edu/policies/softwareauth.html>

3.2.3.4 Authentication for Services Outside the University Environment

NU does not export or bulk transfer identities, passwords or personal information to third parties for authentication or any other purpose, so authentication for outside services (e.g., mixed host, off-campus host, etc.) requires special handling. NetID and password authentication, Web SSO, federated authentication, and web proxy are services that are commonly offered.

Authentication Requirements for University Software Applications Policy
<http://www.it.northwestern.edu/policies/coordinate.html>

3.3 Confidentiality/Privacy

The Northwestern network is owned and operated by the University for its own use for academic, research, and administrative purposes, and all transmissions over the Northwestern network are viewed and treated as private. While the use of the network


and of University computing resources is strictly by permission of the University, and data and communications considered confidential, that confidentiality is not guaranteed. Under certain conditions and with specific approvals, data may be subject to review.

Privacy within the Northwestern Network

<http://www.it.northwestern.edu/policies/privacy-issues.html>

<http://www.it.northwestern.edu/policies/uccpolicy.html>

3.3.1 Secure Handling of Social Security Numbers

Social Security Numbers are “Legally/Contractually Restricted” information and 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 referenced policies. The primary uses and reasons for the continued capture, storage, retention and processing of SSN data are identified and documented in the [Approved Uses of SSNs - Appendix B](#) .

Secure Handling of Social Security Numbers

http://www.it.northwestern.edu/policies/SSN_policy.html

3.3.2 Securing Data - Data Encryption

When properly implemented, encryption provides an enhanced level of assurance that the data, while encrypted, cannot be viewed or otherwise discovered by unauthorized parties in the event of theft, loss or interception. The University offers several solutions for encrypting data, depending upon the business need: full disk encryption encrypts all data on a hard drive, including files, folders and the operating system; and is most appropriate when the physical security of the system is not assured; file and folder encryption offers a more selective approach, and can be used to encrypt files sent via email. NUIT offers a range of encryption solutions to the community.

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

3.3.3 Securing Communications

Secure 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. Any NU system, application, appliance or site that uses the NetID/password combination for purposes of authentication, or that transmits/receives data classified as “Legally/Contractually Restricted” is required to employ secure measures to ensure confidentiality of this data.

3.3.3.1 Certificate Services

The need for parties to communicate securely over an insecure medium such as the Internet spawned the creation of 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. Trusted authorities, known as Certificate Authorities (CA), sign and distribute certificates for use by entities that need to assure identities and/or establish encrypted

communications. NUIT participates in a certificate program that entitles Northwestern to issue unlimited SSL (Secure Sockets Layer) certificates for secure Web servers on the northwestern.edu domain. A secure Web site uses encryption and authentication standards to protect the confidentiality of Web transactions; SSL is a protocol commonly used for Web security. Any member of the University community with a valid Northwestern e-mail address can request an SSL certificate through this program.

Server Certificates: <http://www.it.northwestern.edu/policies/server-cert.html>

SSL Certificates: <http://www.it.northwestern.edu/security/ssl-certificate/>

3.4 Data Integrity

Data integrity refers to maintaining and assuring the accuracy and consistency of **data** over its entire **life cycle**, and is a critical aspect to the design, implementation and usage of any system, which stores, processes or retrieves data. The overall intent of any data integrity technique is the same: ensure data is recorded exactly as intended (such as a database correctly rejecting mutually exclusive possibilities,) and upon later retrieval, ensure the data is the same as it was when it was originally recorded. In short, data integrity aims to prevent unintentional changes to information. NU security mechanisms are selected and implemented to not only provide availability and confidentiality but also integrity of the information at rest, in use and being transmitted.

3.5 Data Backup and Recovery

It is important for those NU representatives responsible for their department's data backup and recovery procedures to deploy measures that are synchronized with those acceptable to NUIT. Backing up data on a regular basis (daily and/or weekly) will lessen the damage caused by the loss or corruption of stored data. NUIT has identified several backup solutions/providers that meet stated requirements, and there are benefits of scale in using a single provider.

Data Backup: <http://www.it.northwestern.edu/security/backup/>

3.5.1 Workstations (desktops, laptops) Backup

NUIT recommends a regular workstation backup strategy. It should be noted that even with the backup procedures listed above, there is still the possibility of a virus infection or hacker compromise.

Central Desktop Data Backup Service

<http://www.it.northwestern.edu/dss/backup-service/index.html>

3.5.2 Portable Memory Devices Backup

Due to their extreme portability and low cost, memory devices are widely used and easily lost or stolen. Encryption is strongly recommended for these devices to prevent the loss of data if they are lost, as well as scanning new devices for malware before using them for storing any sensitive information.

3.5.3 Server Backup

NUIT recommends a regular backup strategy for any local servers used for data storage. It should be noted that even with the backup procedures mentioned in this section, there is still the possibility of a virus infection or hacker compromise. For secure, economical computing resources, NU advises departments to consider the hosting services offered by the main **NU Data Center**: <http://www.it.northwestern.edu/data-centers/>

3.5.4 Enterprise Storage Systems & Tape Libraries Backup

NU provides an off-site data storage service, with a pick up and drop off provided by the vendor. The media retention period (how long it will be stored off-site) is pre-determined by the customer. The routine is established between the two parties and the fees incurred are based upon the frequency of the pick up/drop off service and the number of containers that are needed. To meet data protection audit requirements, a media rotation of grandfather - father - son is generally followed.

Computing Services Guideline for Off-Site Data Protection Storage

<http://www.it.northwestern.edu/policies/storageguide.html>

3.6 Data Computing/Media Reuse/Destruction

NU offers a service to formally dispose of and reuse NU computers and peripherals designed to help NU meet security and the Environmental Protection Agency (EPA) regulations for equipment disposal. NUIT recommends using this no-charge service as it also offers data removal. Equipment with inventory tags (or cost exceeding \$5,000) must be reported to the Accounting Services Equipment Inventory Coordinator when disposed of.

Disposal of NU Computers: <http://www.it.northwestern.edu/policies/disposal.html>

University Services offers a computer and electronic equipment destruction/recycling ("eCycling") program for faculty, staff, students and commercial tenants. In addition to the security concern of ensuring that sensitive data is made unrecoverable, electronic equipment (CD/DVDs, magnetic tapes, portable storage drives/devices) contain materials that can be hazardous to human health and the environment if they are not properly managed.

eCycling: <http://www.northwestern.edu/uservices/office/computer/staff.html>

For equipment acquired using federal funds, you must get approval of Accounting Services for Research and Sponsored Programs (ASRSP) for disposal:

<http://www.northwestern.edu/asrsp>

3.6.1 Data Media Destruction

It is the responsibility of the department or individual in possession of NU owned computer(s) to ensure that data has been properly removed from the hard drives of computers, CD/DVDs, magnetic tapes, portable storage drives/devices before removal or

redeployment of the equipment. Deleting files from a drive or storage media does not guarantee removal of the data, nor does formatting a drive. Data that has been “deleted” without utilizing specific sanitization procedures can be “undeleted” or otherwise made recoverable. Computers must have their hard disk drives sanitized (data overwritten) with software that completes a multiple-pass binary wipe or the drive must undergo physical alteration/destruction to render data unrecoverable.

3.6.2 Software Reuse/Destruction

Most software applications that are to be reused can be uninstalled prior to moving the software to another computer. Microsoft licenses its original Windows operating system to the processor and motherboard of the desktop computer. So, while it is required that all data be erased, it is appropriate to pass on the original Microsoft Operating System installer disk with the computer when it is sold or repurposed to another department. However, any software purchased from the NUIT’s site licensed program (examples include: Microsoft Office, Adobe Photoshop, etc.) must be retained by NU and can be redeployed by the department that originated the purchase. **Note:** This includes operating system upgrades.

3.6.3 Paper Destruction

When you no longer need sensitive data, it is better to dispose of it than continue to account for it. Ensure printed data can’t be recovered by shredding papers containing sensitive data. **Purchasing – Document Management**

<http://www.northwestern.edu/userservices/purchasing/vendors/secure/cintas-document.html>

4.0 ACCEPTABLE USAGE

NU electronic resources are primarily intended for execution of University business, with incidental personal use permitted, subject to University policy and applicable laws and regulations. Users of this equipment are expected to follow NU policies on the safe and secure use of such.

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>

4.1 Standard Workstation Configuration

Workstation computers (desktop or laptop) are constantly subjected to attempted exploits of system and application vulnerabilities. NUIT provides and abides by the documented measures on workstation computers it configures and recommends individual computer owners seriously considering doing the same.

Security Recommendations for Desktop Computers:

http://www.it.northwestern.edu/policies/desktop_security.html

4.1.1 Handling of Compromised Workstations

When a compromised machine is detected, ISS/C may shut off the port to which the computer is connected, or may disable the user's NetID. Once the computer has been rebuilt and brought current, and ISS/C notified, the port and/or NetID will be returned to active status.

4.2 Laptops

As stated in Section 4.1, laptops should be configured with the standard desktop configuration of security applications. In addition, due to their portability, they are vulnerable to inadvertent loss or theft. Encryption is strongly recommended for all laptop hard drives and portable memory devices. Encryption shall be implemented on all laptops that process Internal and Legally/Contractually Restricted data.

4.3 Personal Computers

Personal computers, whether used for University business or not, almost always contain personal information. To help prevent compromise and exposure of personal data, these devices should also be configured with the same security measures identified in Section 4.1.

4.4 Mobile Devices

Mobile devices continue to expand in their popularity and usage, blending the functions of the personal computer and telephone. As these mobile devices replace the role of the traditional computer, they are exposed to an increasing number and sophistication of threats of compromise from malware, theft and loss. Users should configure their mobile devices to use the NU networks, and consult the owner/operator manual to enable the

specific security features, including keeping the mobile device's software and system up to date, using the automatic update features, etc. If available, use anti-viral software for the device, and keep signatures up to date.

Mobile Device Security: <http://www.it.northwestern.edu/policies/mobile-devices.html>

<http://www.it.northwestern.edu/hardware/iphone/iphone-collab.html>

4.5 Servers

Business units or departments with their own subnets and administrators shall install standard security features at the subnet level. NUIT security personnel can scan the servers, Web sites and Web applications for vulnerabilities upon request. See the [Vulnerability Assessment Program](#) for details. These departments would also benefit from having their administrator join the UNITS listserv, the security listservs and the Network User Status Agent (NUSA).

<http://www.it.northwestern.edu/policies/central-web-server.html>

<http://www.it.northwestern.edu/policies/admin-datacenter-hosting.html>

<http://www.it.northwestern.edu/policies/research-datacenter-hosting.html>

<http://www.it.northwestern.edu/network/nusa/>

4.6 Software

It is NU 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, the terms of software license agreements, or other NU policies pertaining to computer software. Software users must abide by all terms of the software license agreement, be aware that computer software is typically protected by copyright, not accept unlicensed software from any third party, and immediately uninstall and remove any software and/or programs that are not licensed or where the licensing agreement has expired.

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

It is important to maintain timely and appropriate action in the identification of relevant patches and system updates, to ensure the ongoing functionality and security of systems and applications, and to minimize the risk of exploitation of recognized and announced vulnerabilities. Where available, it is recommended that users set the automatic software update notification feature.

4.7 Printers, Scanners, Copiers, and Faxes

When considering new or replacement acquisitions, contact [Purchasing Resource Services](#) for recommendations and preferred vendors. Select a device that is configurable and offers security features. Consider having a network firewall installed on your subnet by Telecommunications and Network Services (TNS) and attach all devices to the firewalled subnet. Review vendor documentation for any listing of security-related features and recommendations on secure installation and implementation. Contact your vendor and inquire about equipment upgrades that include security features. Establish a strong administrator password on the device to help defend against attacks and prevent reconfiguration by an unauthorized user.

<http://www.it.northwestern.edu/policies/networked-devices.html>

4.8 Email

Northwestern University provides faculty and staff with a centrally hosted email service, available after activating a NetID. Most students are provided with an @u.northwestern.edu collaboration account upon issuance of the NetID. The procedures for acceptable use of the NU email service are at:

[activation.http://www.it.northwestern.edu/accounts/email/index.html](http://www.it.northwestern.edu/accounts/email/index.html)

<http://www.it.northwestern.edu/policies/electronic-resources.html>

Email is particularly susceptible to attacks from a host of adversarial activities and therefore should be used with the proper cautions and security measures in place. NUIT offers a system for scanning and filtering junk e-mail, and identifying phishing attempts, viruses and malicious high-risk attachments sent to the University community.

Email Defense: <http://www.it.northwestern.edu/security/eds/index.html>

Disk storage on the central email servers is an important resource. Overall server performance, cost of operations and equipment, and performance of individual accounts are all influenced by disk storage. The servers will be operating with consistent limits of 8 GB for email messages within individual accounts. As accounts approach the 8 GB limit, a series of warning messages will be sent. Accounts that reach 8 GB in message space will no longer receive messages until the space is reduced.

<http://www.it.northwestern.edu/policies/inspool.html>

Using your personal mobile phone for email is permitted if the user follows the required security procedures: <http://www.it.northwestern.edu/hardware/iphone/>

5.0 NETWORK SECURITY

The information technology environment at NU can be described as layers of function around a core of central systems and NU data centers/data warehouses. The NU computer network that ties this all together consists of a campus-wide backbone network, local area networks, and many shared computers as well as personal desktop computers.

5.1 Network Service Eligibility

Policy identifies the groups eligible to receive information systems network services from NUIT. Any applicant for network services not described therein should be referred to the vice president for information technology or designee, who will coordinate a decision on that particular case.

5.2 Network User Rights and Responsibilities

Members of the NU community have certain rights as they use its network and services, such as intellectual freedom, safety from threats and privacy.

<http://www.it.northwestern.edu/policies/privacy-issues.html>.

In exchange, there are responsibilities that must be met as part of the privilege of having NU network access. Knowingly violating a network responsibility can cause your network access to be suspended. Violations that also violate federal or state laws can also result in referral to the appropriate legal authority.

<http://www.it.northwestern.edu/policies/responsibilities.html>.

The NUIT Security Office should be notified about violations of copyright laws and NUIT policies, as well as about potential loopholes in the security of any computer systems and networks at NU. Contact the NUIT Security Office at security@northwestern.edu.

5.3 Firewalls

Firewalls are typically categorized as either “Network” or “Host”. A Network Firewall is most often an appliance attached to a network for the purpose of controlling access to single or multiple hosts, or subnets; a Host Firewall is most often an application that addresses an individual host (e.g., personal computer) separately. Both type of firewalls (Network and Host) can be and often are used jointly.

<http://www.it.northwestern.edu/policies/firewall.html>

5.4 Computer and Network Security Requirements

Maintaining your computer at home or at the office is essential to keep it running smoothly and securely, especially when connected to the NU network. A checklist is available to help maintain a safe and problem-free computer.

Security Checklist: <http://www.it.northwestern.edu/security/checklist.html>

5.4.1 Logging-in

All desktop and laptop computers connected to the NU network should have an administrator account that is not used as the regular login account. The password for the administrator account should always be changed from the default.

5.4.1.1 Log-in Attempts

Limiting the number of attempted login tries is an effective mitigator against automated password cracking attacks; it reduces the number of attempts and the time required to conduct a given number of attempts. Where a risk assessment suggests a vulnerability to such attacks, the installation of a login tries counter should be discussed with the network administrator.

5.4.1.2 Log-in Lockout

Login lockout reduces the number of attempts and the time required to execute a given number of attempts. Where a risk assessment suggests a vulnerability to such attacks, a login tries counter should be discussed with the network administrator..

5.4.1.3 Inactivity Log-off

Inactivity log-off is a measure that reduces the likelihood of an unauthorized individual gaining access to your account and/or the NU network should you leave your workstation without logging out. Where a risk assessment suggests a vulnerability to such attacks, short inactivity sessions (e.g., 5 minutes – instituted in the operating system) and network log-off timers (e.g., inactivity >15 minutes) should be considered.

5.4.2 Network Time Protocol

NU provides precise timing capabilities through the following website:
<http://www.it.northwestern.edu/network/ntp/index.html>

5.5 Malware

Symantec Endpoint Protection is Northwestern's licensed software application for protecting your computer against viruses and other malware. It is critical that every NU student, faculty, and staff member installs Symantec, updates patches and virus definitions, and run virus scans daily.

<http://www.it.northwestern.edu/software/sav/index.html>

5.5.1 Anti-Virus

When a desktop is built, all operating system updates and patches should be applied. In addition, operating system updates and patches should be applied regularly. All NU machines should have the Symantec AntiVirus (PC) installed, available from NUIT, and should retain the setting that schedules regular updates of virus definitions from the central server.

Windows: <http://www.it.northwestern.edu/software/sav/win/index.html>

Mac: <http://www.it.northwestern.edu/software/sav/mac/index.html>

5.6 Server Security

A server is either a physical or virtual instance of an autonomous software system intended to connect with and provide services to other computers. Specific requirements for securing servers are provided in the referenced NUIT policies. Deviations from the recommended guidelines should be documented according to each department's own procedures. The end goal is a secure server that meets the functional and business needs of each department.

<http://www.it.northwestern.edu/policies/serversecurity.html>
<http://www.it.northwestern.edu/policies/sysguide.html>

The NUIT Data Centers provides a secure, enterprise-wide, redundant, and adaptable infrastructure for the reliable delivery of mission-critical University systems, and its use is highly recommended for consideration when computing capability is required. Hosting is available for both physical and virtual servers and storage. The data centers offer professional management of computing services, enabling users to focus on their core mission while NUIT focuses on the IT services.

NUIT Data Centers: <http://it.northwestern.edu/data-centers>

5.7 Transmission Security

Sensitive data transmitted from one location to another on a non-secure link is subject to compromise. Secure transport client/server products provide transport-level encryption to protect data in transit between the sender and recipient; this helps ensure delivery without eavesdropping, interception or forgery. This scenario requires the appropriate configuration of a server in order to allow clients to connect in a secure manner. E-mail-specific products integrate encryption into the e-mail client, allowing messages and attachments to be sent in an encrypted form transparent to the user. This is most appropriate for departments whose users require frequent and regular encryption of e-mail communications.

Encryption of Data in Transit:

<http://www.it.northwestern.edu/policies/dataencryption.html>

5.8 Remote Access

Two means of secure remote computing are available to the NU community for accessing certain Northwestern resources from locations off campus.

5.8.1 VPN

Virtual Private Network (VPN) establishes a "secure tunnel" for your computer on the Northwestern network. 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 for a Secure Connection: <http://www.it.northwestern.edu/oncampus/vpn/>

5.8.2 SSL VPN (Secure Sockets Layer Virtual Private Network)

SSL VPN allows users to remotely access restricted network resources via 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. This protocol achieves a higher level of compatibility with client platforms and configurations for remote networks and firewalls, providing a more reliable connection.

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

5.9 Wireless Access

Northwestern's wireless network provides secure, mobile Internet access for faculty, staff, and students from [wireless access points](#) located throughout the Evanston and Chicago campuses. A [guest wireless access is also available](#) that allows for limited Internet connectivity. When searching for available networks, choose **Northwestern**. This secure network does not need VPN and requires a valid NetID to access. [Connect to the Northwestern network](#) from a laptop, smartphone, or other mobile device using wireless access points conveniently located in campus buildings, [residence halls](#), and public spaces including the Norris University Center and the Northwestern University Library. To find a wireless service location, look for the "NU Wireless Access" signs located throughout the Evanston and Chicago campuses or where indicated on the [University's interactive campus maps](#).

Make a Wireless Connection: <http://www.it.northwestern.edu/oncampus/wireless/>

5.10 Secure Web Applications and Coding

Secure coding practices, in conjunction with pre-production and ongoing testing via ISS/C's Information Security Vulnerability Management and Web Application Assessment Programs, help to ensure that applications are developed and maintained with a minimum exposure to known security vulnerabilities. Developers should utilize the Online Web Application Security Project "[OWASP Top Ten](#)" list to guide their secure coding efforts. The OWASP Top Ten details the most common web application security vulnerabilities, including basic methods to protect against these vulnerabilities. <http://www.it.northwestern.edu/policies/webapps.html>.

Services delivered from mixed host 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: <http://www.it.northwestern.edu/policies/coordinate.html>

5.10.1 Web Assessments

For web application assessment, ISS/C uses an automated Web application and Web services vulnerability assessment tool that is specifically designed to assess potential security flaws and to provide all the information needed to fix them. As an assessment is initiated, the tool assigns "assessment agents" that dynamically catalog all areas of a Web application. As these agents complete the assessment, findings are reported to a main security engine that analyzes the results. The tool then launches audit engines to evaluate the gathered information and apply attack algorithms to locate vulnerabilities and

determine their severity. Manual assessments are also possible for in-depth testing.
<http://www.it.northwestern.edu/security/vulnerability.html>

5.11 Accountability

As stated in Section 5.2, the NU community can expect certain rights as they use its network and services; and network users are held accountable for their network actions.

5.11.1 Activity Monitoring

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

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

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

5.11.2 Computer, System, or Network Monitoring

NU reserves the right to take whatever steps are necessary to investigate possible network security threats, to investigate suspected violations of NU regulations, or to assist appropriate authorities to investigate suspected illegal activities.

5.11.3 Data Search Utilities

NUIT has tested and recommended data search tools, and may provide preventative and remedial measures for locating sensitive data on NU desktop computers. For every tool, make sure that it checks all possible files that may contain sensitive data, and be aware that PDFs and ZIP files may cause problems, though these formats may contain sensitive data. Technical support staff should also have knowledge of how to create searches with wildcard and other character strings for SSNs and credit card numbers. [A short reference about character string searching](#) is available from NUIT Information and Systems Security/Compliance: <http://www.it.northwestern.edu/policies/datasearch.html>

6.0 PHYSICAL SECURITY

Physical security encompasses personnel, facility, and IT equipment security. Personnel and facility security are primarily handled by the NU Police Department (UP)

<http://www.northwestern.edu/up/> and Facilities Management (FM)

<http://www.northwestern.edu/fm/>.

6.1 Facility Security Plan

6.1.1 Physical Access Controls

Facilities management controls the various keys, card, and biometric access readers.

6.1.1.1 Entry Control

A variety of entry control options are available depending on the level of security, access control and access monitoring required.

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

6.1.1.2 Physical Security Access Control for Data Center Visitors

Due to the large volume of information contained in the NU data centers, strict physical access control security measures are in place. Employees are required to wear photo ID badges and must pass two and three factor authentication.

Data Center Security: <http://www.it.northwestern.edu/data-centers/index.html>

6.1.2 Environmental Controls

Facilities Management is in charge of maintaining the environmental controls (HVAC, fire protection, etc.) and power for all facilities. Individual building users are responsible to coordinate with FM for IT equipment cooling and uninterruptible power supplies.

<http://www.northwestern.edu/fm/services/operation-and-maintenance-services/engineering.html>. The data centers have their own environmental control

personnel to support the extensive controls they have in place.

<http://www.it.northwestern.edu/bin/docs/datacenter-brochure-2012.pdf>

6.1.3 Facility Maintenance Records

Maintenance records should be kept to determine if adequate maintenance on security-related features is being performed.

6.2 Physical Security and Incident Reporting

University Police provides a full range of services 24 hours a day, 365 days a year. The department has the primary responsibility for crime prevention, law enforcement, parking control, emergency preparedness/response and security at special events.

University Police: <http://www.northwestern.edu/up/index.html>

6.2.1 Incident Handling/Responding

Campus Police provide a means to report physical security/crime reports.

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

6.3 Emergency Mode Operation

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

6.3.1 Emergency Physical Access Control

All NU facilities have emergency egress routes posted.

6.3.2 Emergency Access to Data

Departments that maintain large amounts of data processing capabilities should include in their emergency planning, ways to protect and regain access to data in times of emergencies.

6.4 Disaster Recovery/Business Continuity Planning

A disaster is defined as a major disruption to normal processing due to physical damage to the equipment or facility or the inability to access or process IT at the facility. Only the NU Vice President of IT or the Associate Vice President of IT are authorized to activate the Disaster Recovery Plan (DRP). The IT DRP is a subset of the overall DRP and is developed in collaboration with the Office of Financial Operations Business Continuity Department; it is meant to restore critical IT facilities (e.g., key applications, the data centers) and to resume at least the most critical of services as quickly as possible following a disaster. The Business Continuity portion of the plan provides the processes and actions to follow to resume processing in a reduced capability mode, possibly even at an alternate site if required. The plan calls for for an organized assessment of damages to the facilities and equipment, as well as the means for timely executive decisions regarding restoration of the facilities. It should include an evaluation of how to establish temporary operations under likely emergency situations, a call list for all personnel, etc. For example, a typical restore process could follow the following sequence:

- a. Restore Disk Drives from backups
- b. Bring up the Operating systems
- c. Restore the databases
- d. Bring up data communications systems

Emergency Management Operations:

<http://www.northwestern.edu/up/emergency/overview.html>

Business Continuity Planning Template

www.northwestern.edu/bcp/documents/nu-bcp-template.docx

6.4.1 Applications and Data Criticality Analysis and Ranking

Based on the established value to the given department/business units operations, a ranked list of data applications shall be established to represent the order in which the facilities would be brought back up. In this case, the value equates to the level of necessity to the essential business operations of the University. In time of emergency, it may be necessary to allocate resources (e.g., limited amount of emergency backup power) to the most necessary operations first.

6.4.2 Evaluation of Contingency Plans

Periodically, the Disaster Recovery Team should meet to review the DRP for currency and modification.

6.4.3 Testing Contingency Plans

Contingency plans should be tested on a yearly basis, in at least an organizational level, i.e., involving all appropriate managers to be involved in a disaster scenario drill.

7.0 PERSONNEL SECURITY AND HUMAN RESOURCES

7.1 Hiring

Northwestern University is committed to employing qualified talent and providing a safe environment for all employees and students. <http://www.northwestern.edu/hr/>

7.1.1 Recruiting and Hiring Procedures

Individuals who have been selected as final candidates for staff positions must successfully complete a background check prior to beginning employment in their new position. Additionally, upon accepting the new position, these individuals must sign an acknowledgement of their status as a mandated reporter which indicates the employee understands that he or she is required to make a report to the Illinois Department of Children & Family Services (DCFS) Hotline whenever there is reasonable cause to believe that a child known to them in their professional or official capacity may be abused or neglected. Both of these processes apply to:

- a. Individuals who are new to the University in staff positions
- b. Existing staff employees who transfer or who are promoted into a new position
- c. Temporary employees

7.1.2 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 hired through the University's Temporary Center. Background checks, education verification, identity verification, and reference checks are conducted in accordance with applicable privacy and data regulations and include the following:

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

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

7.1.3 Business Associates and 3rd Parties

Business associates and third parties represent a greater risk to the University as they have a different set of motivations and goals than a university employee. Under many laws, a Business Associate is treated as an employee for issues of liability, etc. and so they should be made aware of and held accountable for all applicable policies and responsibilities of the systems they are involved with. All contracts with either group should be processed through the office of the General Counsel.

7.2 Terminations and Transfers

Terminating 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. Notification shall be made to department management and Human Resources. If termination of employment is recommended for individuals in regular staff positions, the supervising staff or faculty member discusses the situation with the Human Resources Consultant to determine the appropriate action and receive approval for termination if appropriate. When regular staff members are involuntarily terminated for cause, the HR Consultant notifies ISS/C to immediately disable the staff member's Net ID. Human Resources also oversee the transfer process for employees in regular staff positions. Long standing employees can amass a large number of unneeded privileges on systems they no longer access if the privileges are not deleted when they make transfers, which can represent a window of opportunity for a criminal attacker. The Temporary Center coordinates with the department regarding the termination of any temporary employees processed through the Temporary Center.

7.2.1 Procedure for Exiting Employees

Employees must return to the department any University property, materials, and written information issued to them or in their possession on or before the last day of work, including credit cards, identification badges or cards, keys, manuals, calculators, computers, other 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](#) for departments to utilize when staff members transfer or exit the organization.

- a. For transfers and other instances where the separation is under amicable terms (e.g., contract expiration), you should:
 - i. Consider monitoring access until employment or contract service expires (end date);
 - ii. Reduce access to only those resources and facilities required to fulfill any remaining obligations or work activities through the stated end date;
 - iii. Remove all access to sensitive data and facilities as of the end date.
- b. For instances where termination is for cause, remove access to all resources and facilities immediately.

7.3 Sanctions

Violations of these policies 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 Faculty, Staff, and Student Handbooks, the Standards of Business Conduct, and via contractual agreements with third parties doing business with the University. <http://www.it.northwestern.edu/policies/responsibilities.html>

7.3.1 Security Breaches

Northwestern University policies related to technology are created to ensure a productive and safe environment for the University community. Taking on many forms, violations of these policies open the University to a host of legal and information security risks. Some examples include:

- a. The addition of equipment that extends the University network (hub/hublets, repeaters, and wire access points)
- b. Violation of copyright laws, such as illegal file-sharing and/or downloading of audio and/or video files
- c. Password sharing (e.g., University NetID password)
- d. Improper use of University technology resources
- e. Accepting charge cards on unapproved University websites
- f. Information privacy violations (downloading and/or allowing access to sensitive/private information)
- g. Illegal computing activities (e.g., virus/worm creation, hacking)

To report a violation of NUIT policy, follow the instructions at:

<http://www.it.northwestern.edu/policies/reporting.html>

7.4 Security Training and Awareness

The NUIT Communications team continues to partner with ISS/C to strengthen NUIT'S computer and network security efforts. In addition to creating focused communication that segments the specific audiences of the NU community, the NUIT Communications team maintains the most essential security-related information on its website:

<http://www.it.northwestern.edu/security/index.html>

7.4.1 New Hire

Security podcasts (audio and video), anti-phishing program news articles, Tech Talks, etc. are available on the NUIT website:

<http://www.it.northwestern.edu/learning/index.html>

7.4.1.1 Employee Orientations (New and Existing)

NUIT has a full complement of training materials available to new, as well as existing, employees. Human Resources includes introducing the NU IT capabilities as part of their indoctrination process:

Security Awareness: <http://www.it.northwestern.edu/transitions/2005/key.html>

7.4.2 Recurrent Training

Recurrent training is not tracked by NUIT, but it's recommended that the individual and departments keep track of current educational activities by monitoring the podcasts, security tips, and information documentation produced by NUIT ISS/C.

7.4.3 Security Reminders

Security reminders are posted periodically and any time that an incident requires notification of the university community:

Podcasts: <http://www.it.northwestern.edu/security/podcast.html>

eCommunicator: <http://www.it.northwestern.edu/news/publication/ecommunicator.html>

8.0 INFORMATION SYSTEMS CONFIGURATION MANAGEMENT

8.1 Information Technology Acquisition, Development and Deployment

NUIT is the major consultative resource for division and school IT workforce and end-users for all IT systems including communication systems, information storage and processing systems, software systems, physical facilities related to such systems and contractual relationships with vendors of such systems and services. In addition, NUIT has oversight and coordinating responsibility for all these systems and services. All acquisitions and deployments of IT within NU must conform to NU guidelines to maximize functionality while minimizing effort and be reviewed with NUIT.

Technological innovations and initiatives within the divisions and schools should be brought to NUIT early in their life for rapid consideration and assessment within NU-wide plans. Because any new idea or approach may benefit or hamper others, NUIT, in collaboration with school or division IT workers, will expeditiously work with the end-users to review their initiatives to insure that all acquisitions, development, and deployments of IT within NU conforms to existing guidelines to maximize functionality while minimizing effort.

All members of the NU community must consult with NUIT before developing, purchasing or contracting for IT products, vendor services, support or consulting. In general, individual IT acquisitions should be coordinated within the school or division by the designated technology leader. That person will have knowledge of how particular proposals will fit within the school or division strategy. The school or division may also establish its own guidelines for review in concert with the central policy and guidelines. The technology leader is regularly briefed by NUIT and can determine if a proposal will require NUIT review or approvals, and if so contact the Associate Vice President in the Office of the Vice President for Information Technology and submit a brief description of the project, product, or service, complete financial information including anticipated or approved funding sources, vendor product specification documentation and, if applicable, any relevant contracts or agreements. Authentication of users is performed using the NetID and its associated password. This requirement should be included in all bid specifications when acquiring applications.

<http://www.it.northwestern.edu/policies/guidelines.html>

<http://www.it.northwestern.edu/policies/acquisition.html>

http://www.northwestern.edu/userservices/purchasing/vendors/ibuynu_marketplace.html

8.2 Configuration Management

All NU-owned or issued and any personally-owned computer or related equipment (e.g., server, workstations, laptops, PDAs, printers, fax, and other such devices) that can be connected to the NU network, or is used to capture, process or store NU data, or is used in the conduct of NU business should be tracked in an inventory tracking system that identifies its serial number, location, and ownership as a minimum. Computing equipment and data media should be identified as to the level of classification of the data it contains. Equipment with inventory tags (or costs exceeding \$5,000) must be reported to the Accounting Services Equipment Inventory Coordinator.

8.2.1 Networks

The communications infrastructure of the University is a critical strategic advantage that facilitates teaching, research, and administration. The policies in place ensure that the University deploys a consistent infrastructure (wired, wireless, video, voice, converged communications) to NU 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. Any transmission facilities, or network-attached computing technologies, that are to be acquired with capital project funds, must be reviewed and approved by NUIT during planning. <http://www.it.northwestern.edu/policies/coordinate.html>

8.2.1.1 NU-Owned Building Infrastructure

Any NU organizations in NU-owned buildings receive network facilities (voice, data, and video services) provided by and coordinated with NUIT and NU Facilities Management (FM).

8.2.1.2 NU Non-University owned Building Infrastructure

Any NU organization that moves to a non-NU owned building will receive the same network facilities (voice, data, and video services) that are delivered in NU-owned buildings, as provided by and coordinated with NUIT and NU Facilities Management (FM). Any NU affiliate that wishes to receive NUIT services will be held to the same standards as a NU department. NUIT will determine the suitable infrastructure, contract and coordinate for installation thereof, and, based on the funding identified, charge the customer organization or the project budget accordingly.

<http://www.it.northwestern.edu/policies/infrastructure.html>

8.2.2 Servers Configuration Management

Server configuration is dictated by the hosting facility and should follow the guidelines used by the NU Data Centers for their hosting service.

<http://www.it.northwestern.edu/policies/sysguide.html>

8.2.3 Software Configuration Management

Computer software is a major form of intellectual property, both from the standpoint of the intellectual creativity required to produce it and the practical and commercial value of good products. Buying or using software subjects both the individual and NU to legal obligations, as well as to legal risks if the software is used improperly. All software used for NU purposes should be configuration controlled. Any changes to software configurations (commonly called patches) should be tracked. To reduce the risks resulting from possible exploitation of recognized (published) technical vulnerabilities, security patches should be kept up to date.

8.2.4 Workstations Configuration Management

Individual departments are granted quite a bit of purchasing freedom for workstations, but it is in the best interests of all parties to follow the NUIT standard configurations identified in Section 4, and by Distributed Support Services, to maintain a consistent level of security and compatibility. Workstations should be identified as to the level of the highest classification of the data they may contain/process, and handled appropriately.

8.2.5 Portable Devices Configuration Management

Individual departments are granted quite a bit of purchasing freedom for laptops, but it is in the best interests of all parties to follow the NUIT standard configurations identified in Section 4, and by Distributed Support Services, to maintain a consistent level of security and compatibility. They should be identified as to the level of the highest classification of the data it may contain/process, and handled appropriately.

8.2.6 Devices and Media Accountability

Devices and data media should be identified as to the level of classification of the data they contain/process. The marking of devices that contain sensitive data is a best practice and strongly recommended.

8.3 Configuration Change Control

The purpose of the Change Management implementation at Northwestern University is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes associated with the University's IT infrastructure and services, in order to minimize the number and impact of any related incidents. Changes in the IT infrastructure may arise reactively in response to problems, or proactively from seeking improved efficiency and effectiveness, as well as to enable or reflect business initiatives, programs, projects, or service improvements.

8.3.1 Change Approval Board (CAB)

The Change Approval board (CAB) delivers support to the Change Management team by approving requested changes and assisting in the assessment and prioritization of changes. This body is generally made up of IT representatives that include: the Change Manager, User managers and groups, technical experts, and possible third parties (if required). CAB meetings will be held at regularly scheduled intervals, typically weekly. A CAB offers multiple perspectives necessary to ensure proper decision-making. For example, a decision made solely by IT may fail to recognize the concerns of accounting. The CAB is tasked with reviewing and prioritizing requested changes, monitoring the change process and providing managerial feedback. A CAB is an integral part of a defined change management process designed to balance the need for change with the need to minimize inherent risks. The CAB is responsible for oversight of all changes in the production environment. As such, it has requests coming in from management, users and IT. The changes may involve hardware, software, configuration settings, patches, etc.

Change Approval: http://wiki.it.northwestern.edu/wiki/index.php/Process_Reports

8.3.1.1 Submitting a Change Request

The person or group responsible for the implementation of a change has the responsibility of documenting and submitting the Change Request. Prior to preparation of a Change Request, all technical aspects of a change should be coordinated between the Requester and the personnel whose responsibility it will be to implement the change. Changes should be tested prior to implementation and information regarding the success/failure of tests included in the Change Request.

Change Request: http://wiki.it.northwestern.edu/wiki/index.php/Service_Catalog

9.0 PAYMENT CARD DATA PROTECTION

The Payment Card Information (PCI) data security standards (DSS) apply to all entities that store, process or transmit cardholder data. The standards were developed by the industry itself, based around accepted data security best practices. All NU departments that accept credit card payments must process those payments in a manner compliant the standards. As part of its information security architecture, NUIT has instituted many of the technical measures in the PCI DSS. NUIT will provide technical guidance and coordinate the deployment of required equipment on a case-by-case basis for groups wishing to process credit card payments, but as a rule it is best left to outside vendors to handle.

9.1 eCommerce Operations

NU eCommerce Operations under the auspices of Treasury Operations directs a compliance program as an extension of managing merchant identification numbers. Participation in the PCI compliance program is mandatory for all NU merchants. Failure to fully participate in the program may result in your Merchant ID being revoked.

9.2 Annual Self-Assessment Questionnaires

All merchants are required to complete a self-assessment questionnaire (SAQ) at least annually. A separate questionnaire must be completed for each merchant ID.

9.3 Conducting SAQs

Treasury Operations maintains a contract with an outside vendor to administrate SAQs. All SAQs should be completed through the vendors website.

9.4 PCI Firewalls

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. NU organizations requiring PCI/DSS compliance should contract with a PCI-compliant vendor to operate network equipment that falls within PCI/DSS scope and requirements. NUIT will provide technical guidance and coordinate the deployment of required equipment. PCI/DSS Firewalls should include the use of Network Address Translation (NAT) where required to help ensure compliance with PCI/DSS. Any questions about the suitability and use of NAT should be directed to ISS/C.

Merchant Card Processing: <http://www.it.northwestern.edu/policies/ecommerce.html>

10.0 INFORMATION SYSTEMS (IS) SECURITY RISK MANAGEMENT

10.1 IS Security Risk Identification

The IS risk management program is part of the overall NU Enterprise Risk Management (ERM) program and has as its purpose to prevent, detect, contain, and correct both deliberate and inadvertent IT security incidents. Using various analytic efforts, NUIT ISS/C identifies and ranks risks in order of total overall risk. All IT security projects should be evaluated in terms of the risk vs. costs to further mitigate that risk, prior to making a final decision on expenditure of funding. The IT risk profile is divided into the following categories.

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

IT Risk Assessment and Management Policy (proposed new policy)

10.1.1 Deliberate Attacks

These are the attacks that are likely to be initiated in a planned, deliberate manner. Attackers motivation and sophistication is varied, but generally falls into one of the categories of: disgruntled employees, hackers, vandals, criminals, organized crime, and nation-states. With the large amount of intellectual, healthcare-related, and research data that is contained in university information systems, the likelihood of deliberate attacks against NU must be assumed to exist and be planned for.

10.1.2 Accidental/Inadvertent Incidents

NU information systems are designed to minimize the likelihood of unintentional occurrences that introduce errors, compromises or vulnerabilities into the systems. Risk efforts are focused on identifying such potentials and policies are instituted that attempt to reduce their likelihood, e.g., security awareness efforts.

10.1.3 Emergencies

Risk management activities also include efforts to determine the types of natural phenomena that NUIT facilities are likely to experience over their operating lifetime and how the designs and procedural measures in place would deal with such. The goal is to maintain security while minimizing the damage or loss of information and information systems in all conceivable credible abnormal environments, e.g., fires, flooding, earthquakes, etc. NUIT is a member of the Business Continuity Planning programs.

10.2 IS Security Risk Analysis/Ranking

After potential IS risks are identified, analyses on the risks are conducted to prepare an accurate and thorough assessment of their impacts on the confidentiality, availability, and integrity of university sensitive information. This effort also provides the information to rank risks in order of their likelihood to happen, likelihood of success if attempted, and the consequences of their occurrence. The risks will be defined in a format compatible with that used by the Risk Initiative Steering Committee (RISC) that supports the ERM program and the efforts conducted by Audit and Advisory Services. The ISS/C group

supports this effort with vulnerability assessment services, which are available to the NU community.

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

10.2.1 Information Systems Activity Reviews

Security reports are provided by ISS/C on at least a quarterly basis for management review. Where the need is identified, vulnerabilities will be presented to the ERM committee.

10.3 IS Security Risk Mitigation

Using the risk-related information generated in the efforts described above, NUIT implements a combination of policy, procedures, and physical measures to sufficiently reduce (mitigate) the vulnerabilities and risks to a reasonable level in compliance with NU, customer, and governmental requirements, and NU-adopted standards.

10.4 IS Risk Reevaluation

10.4.1 IS Self-Audits and Activity Reviews

NUIT's ISS/C is constantly monitoring the identified NU IT risk profile to measure and refine its effectiveness. The NU Auditing and Advisory Service conducts audits on a periodic basis that include the IT systems: <http://www.northwestern.edu/audit-and-advisory/services/risk-and-control/erm.html>

10.4.2 IS External Audits

Audits focused specifically on information systems are occasionally conducted by outside organizations that specialize in risk assessment.

10.5 IT Security Incident Response and Reporting

An Incident Response Protocol is in place to address instances of unauthorized access to or disclosure of NU information systems/data. The process 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, while minimizing the adverse impact to the NU.

10.5.1 IT Incident Response Team

Central to this process is the Incident Response Team (IRT), assembled with the purpose of addressing that particular circumstance where there is credible evidence of an incident. The IRT is chaired by the Director of ISS/C and composed of members from all relevant NUIT departments. The process to follow is documented in the Incident Response policy.

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

11.0 DEFINITIONS

Following are a few key definitions of terms used in this document.

Term	Definition
Certificate Authority (CA)	An authority in a network that issues and manages security credentials for message encryption.
Certificate, also Digital Certificate	An electronic document used to bind together a public key with an identity.
Data Steward	The individual(s) responsible for the administration and access to information applications.
Enterprise System	Applicable to any infrastructure as a means of describing its importance to the University's mission and how it should be administered, protected, and funded. From a functional viewpoint, an Enterprise System will be either (a) the only delivery platform for an essential service, or (b) a platform for a service to be a very broad constituency spanning organizational boundaries. An Enterprise System is most frequently administered and protected by an institutional unit with expertise in both the technology and the business functions delivered.
Firewall	Any hardware and/or software designed to examine network traffic using policy statements (ruleset) to block unauthorized access while permitting authorized communications to or from a network or electronic equipment.
Firewall Administrator	The University function charged with the responsibility of Firewall Configuration and/or Ruleset administration. Administrative duties typically include implementation and documentation of approved changes, analysis of activity logs, and execution and documentation of reviews of system settings and/or rulesets.
Firewall Configuration	The system settings affecting the operation of a firewall appliance.
Firewall Ruleset	A set of policy statements or instructions used by a firewall to filter network traffic.
Host	Any computer connected to a network.

Term	Definition
Host Firewall	A firewall application that addresses a separate and distinct host. Examples include, but are not limited to: Symantec's Norton Personal Firewall, Zone Labs' ZoneAlarm, native firewall functionality supplied under operating systems, e.g., Mac OS X, Linux, Windows XP SP2 (and higher). Information that is intended for use by and made available to members of the University community who have a business need to know. This information is not restricted by local, state, national, or international statute regarding disclosure or use.
HTTPS	A combination of the Hypertext Transfer Protocol (HTTP) with the SSL/TLS protocol to provide encryption and secure identification of the server.
Legally/Contractually Restricted:	University information that is required to be protected by applicable law or statute (e.g., HIPAA, FERPA, or the Illinois Personal Information Protection Act), or which, if disclosed to the public could expose the University to legal or financial obligations.
Network Device	Any physical equipment attached to the University network designed to view, cause or facilitate the flow of traffic within a network. Examples include, but are not limited to: routers, switches, hubs, wireless access points.
Network Extension	Any physical equipment attached to the University network designed to increase the port capacity (number of available ports).
Network Firewall	A firewall appliance attached to a network for the purpose of controlling traffic flows to and from single or multiple hosts or subnet(s).
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Removable or Transportable Media	Includes but is not limited to paper forms, reports, cassettes, CDs, USB tokens, flash drives, hard drives and zip drives.
SSL/TLS, also Secure Socket Layer and Transport Layer Security	Protocols used to authenticate servers and clients and to encrypt messages between the authenticated parties.
University Network	The network infrastructure and associated devices provided or served by the University.
Wildcard Certificate	Allows you to secure multiple sub domains on one domain on the same server using *.domain.com pattern for the common name.
Workstations	Includes but is not limited to desktops, laptops, tablets, smart phones and PDAs.

12.0 APPLICABLE REQUIREMENTS

The requirements contained in this document are based on the following laws, regulations, requirements, and guidelines; with a tailoring to NUs unique environment. This means that some IT ‘ recommended practices’ will receive more emphasis than others, based on the specific issues that NU risk assessments have identified.

12.1 NU Information Technology, Technology-Related Policies

Available on the various links provided herein to NU websites.

12.2 Health Insurance Portability and Accountability Act (HIPAA) Security Rules and the 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) that exists in numerous processing facilities on the NU campuses, and is the primary concern for NUIT. HIPAA security standards are listed as ‘Required’ and ‘Addressable’. Required standards must be adopted and Addressable must be evaluated for adoption, based on the risks involved.

12.3 National Institute of Standards (NIST) – guidance only

Identifies the information security standards established by the U.S. government.

12.4 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 guides for specific requirements.

12.5 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.

12.6 ISO Information Security Standards

Identifies the internationally approved standards that could be considered the most overarching of all IT requirements. These standards are the basis of the NU IT information security architecture. Appendix One contains a tracing of the NU policies to the ISO Information Security Standard 27002.

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

12.8 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.

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

The objective of the standard is to establish an industry consistent level of information security controls on credit card data to prevent credit card fraud.

APPENDIX ONE

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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU 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
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
The organization shall maintain a security policy framework.	5.1 Information Security Policy		NUIT Strategic Plan	NU 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
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
Organization has assigned responsibility for security to an individual or committee.			NUIT Organization	2.0 NUIT Organization

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
Organizations will maintain current organizational charts	6.1 Internal organization		NUIT Website	2.0 NUIT Organization
Management will show commitment to the security program and its efforts	6.1.1 Management commitment		NUIT Strategic Plan	2.0 NUIT 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
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
Procedures will be in place that requires 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
The organization will utilize confidentiality agreements to protect its information resources.	6.1.5 Confidentiality agreements		Confidentiality, Non-Disclosure Agreements	3.1 Information Classification
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
The organization utilizes SME advice for the new projects or major program changes.	6.1.7 Specialist security advice		Consulting Contracts	

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
Maintain security of the organization's information and information processing facilities from external parties	6.2 External parties			6.2 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
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU 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
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
Media is labeled so it can be identified by a classification.	7.2 Information Classification		Data Access Policy	8.2 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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
Management's responsibilities to technology and security are clearly defined.	8.2.1 Management responsibilities		NUIT Website	2.0 NUIT Organization
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
Implement a disciplinary process for employees that commit a security breach.	8.2.3 Disciplinary Process	Sanction Policy §164.308(a)(1)	HR website NU Staff Handbook	7.3 Sanctions 7.3.1 Security Breaches
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
<p>Organization has procedures for terminating access to electronic information when the employment of a workforce member ends.</p> <p>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.</p>	<p>8.3.1 Termination Responsibilities</p> <p>8.3.2 Return of Assets</p> <p>8.3.3 Removal of Access Rights</p>	<p>Termination Procedures §164.308(a)(3)(ii)(C)</p>	<p>Employment Termination Checklist</p> <p>NU Staff Handbook</p>	<p>7.2 Terminations and Transfers</p>
<p>Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.</p> <p>Maintain strict control over the internal or external distribution of any kind of media that contains cardholder information.</p>	<p>9.1.1 Physical security perimeter</p>	<p>Facility Security Plan §164.310(a)</p>	<p>NU Police Department Policies</p>	<p>6.1 Facility Security Plan</p>
<p>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.</p>	<p>9.1.2 Physical entry controls</p>	<p>Access Control and Validation Procedures §164.310(a)</p>	<p>NU Police Department Policies</p> <p>NUDC SOP (Data Center)</p>	<p>6.1.1 Physical Access Controls</p>
<p>Access to the data center, computer room, and sensitive areas of the operations center is controlled through electronic key cards assigned to appropriate employees.</p>	<p>9.1.3 Secure offices, rooms, and facilities</p>		<p>NUDC SOP (Data Center)</p>	<p>6.1.1.1 Entry Control</p>
<p>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.</p>	<p>9.1.4 Protecting against external and environment</p>		<p>NUDC SOP (Data Center)</p>	<p>6.1.2 Environmental Controls</p>

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU 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
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 siting and protection	Facility Security Plan §164.310(a)	NU Police Department Policies NUDC SOP (Data Center)	6.1.1 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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
Management approves all media that is moved from a secure area (especially when media is entrusted 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
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
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
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
Change control procedures will be followed for changes in infrastructure.	10.1.2 Change Management		Change Management Process Handbook	8.3 Configuration Change Control
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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 3 rd party service delivery – contract	Business Associate Contracts and Other Arrangement §164.308(b)		3.1 Information Classification 7.1.3 Business Associates and 3 rd 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 3 rd party monitoring and review	Business Associate Contracts and Other Arrangement §164.308(b)		3.1 Information Classification 7.1.3 Business Associates and 3 rd Parties
Organization has policies and procedures for managing the changes involving 3 rd parties.	10.2.3 Managing changes to 3 rd party services	Business Associate Contracts and Other Arrangement §164.308(b)		7.1.3 Business Associates and 3 rd Parties
Organization conducts capacity planning on production systems.	10.3.1 Capacity planning		NUIT Strategic Plan	2.2 NU Information Technology
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
<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.</p> <p>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.</p>	11.1.1 Access control policy	Information Access Management §164.308(a)(4)	Data Access NetID and Network Privileges	3.2 Data Access Management
<p>Limit access to computing resources to only those individuals whose job requires such access.</p>	11.2 User access management	Information Access Management §164.308(a)(4)		3.2.1.3 Changing Information Access Authorizations
<p>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).</p>	11.2.1 User registration	<p>Access Authorization §164.308(a)(4)</p> <p>Unique User Identification §164.312(a)</p>	Net ID and Password Security	<p>3.2.1.1 Eligibility for Information Access</p> <p>3.2.3 Workforce Member Authentication</p>
<p>Implement policies and procedures for granting access to electronic assets. For example, through access to a workstation, transaction, program, process, or other mechanism.</p> <p>Ensure proper user authentication and password management for non-consumer users and administrators, on all system components.</p>	11.2.2 Privilege management	Access Authorization §164.308(a)(4)	Net ID and Password Security	3.2.3 Workforce Member Authentication

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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
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
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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			
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU 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
Users will be authenticated using industry standards, best 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
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
System utilities will only be used if authorized and are 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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
Applications define controls around information accessed inside the application.	11.6.1 Information access restriction	Access Establishment and Modification §164.308(a)(4)		
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
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
Synchronize all critical system clocks and times	10.10.6 Clock synchronization			5.4.2 Network Time Protocol

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
Develop applications based on secure coding guidelines and business requirements.	12.1 Security requirements of information systems			
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
Application will validate data being submitted to the system to check for validity.	12.2.1 Input data validation			3.4 Data Integrity
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
Applications will validate the data being presented as output to ensure the data is correct.	12.2.4 Output data validation			

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.	12.4 Security of system files			
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			
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 difficult to later and requires authorization to 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
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
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
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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU 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
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
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
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
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
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. Off-site facilities are mandatory?	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
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

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
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
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
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
Compliance with Legal Requirements, Security policies, auditing controls	15.1 Compliance with legal requirements		NU General Counsel website	12.0 Applicable Requirements
	15.2 Compliance with Security policies	Evaluation §164.308(a)(8)	Vulnerability Management Program website	10.2 IS Security Risk Analysis/Ranking

ISO Control Description	ISO 27002	HIPAA	NUIT Policy	NU ISSP/P
	15.3 Information systems audits		NU Auditing website	10.4.1 IS Self-Audits and Activity Reviews