University at Buffalo
The State University of New York

Data Risk Classification Policy

Category: Information Technology
Responsible Office: Vice President and Chief Information Officer
Responsible Executive: Vice President and Chief Information Officer

Date Established: 05/24/2010
Date Last Updated: 11/28/2017

Summary

UB classifies its data into three risk-based categories to determine who is allowed to access the data and what security precautions are required to protect the data. This policy facilitates applying the appropriate security controls to university data and assists data trustees in determining the level of security required to protect data.

Policy Statement

The University at Buffalo (UB, university) is committed to protecting the confidentiality, integrity, and availability of data important to the university's mission. All university data must be classified based on risk category and protected using the appropriate security measures consistent with the minimum standards for the classification category. The standard for protecting the data becomes more stringent as the risk from disclosure increases.

DATA CLASSIFICATION				
Data Risk Classification Category	**Minimum Security Standard, per National Institute of Standards and Technology**	**Risk from Disclosure**	**Definition**	**Examples**
Categorization and *Risk from Disclosure* levels use the Federal Information Processing Standards (FIPS) 199				

DATA CLASSIFICATION				
Data Risk Classification Category	**Minimum Security Standard, per National Institute of Standards and Technology**	**Risk from Disclosure**	**Definition**	**Examples**
Category 1- Restricted	800-53-I	High	Protection of the data is required by law/regulation. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation. Restricted data includes the definition of private information in the *New York State Security and Breach Notification Act* as a foundation: bank account/credit card/debit card numbers, social security numbers, state-issued driver license numbers, and state-issued non-driver identification numbers. To this list, the university policy adds protected health information (PHI) as defined and regulated by HIPAA, computer passwords, other computer access protection data, and passport numbers. Category 1- Restricted data are exempt from disclosure/release under the *New York State Freedom of Information Law* (FOIL). The *Information Security Breach and Notification Act* requires the university to disclose any breach of the data to New York residents. (State entities must also notify non-residents, see the *New York State Information Security Policy*.) Individuals who access, process, store, or in any other way handle Category 1- Restricted data are required to implement controls and security measures as required by relevant laws and/or regulations in addition to any university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation should be enacted.	- Social security number (SSN) - Driver license number - State-issue non-driver ID number - Bank/financial account number - Credit/debit card number (CCN) - HIPAA regulated PHI in any form (oral, paper, electronic) - Passport number - University IT authentication credentials - Documents protected by attorney-client privilege - Donor contact information and non-public gift information
Category 2- Private	NIST 800-53-II	Moderate	Includes university data not identified as Category 1- Restricted data, but includes data protected by state and federal	- FERPA-protected data - *Gramm-Leach Bliley* data

DATA CLASSIFICATION				
Data Risk Classification Category	**Minimum Security Standard, per National Institute of Standards and Technology**	**Risk from Disclosure**	**Definition**	**Examples**
		🟧	regulations. This includes Family Educational Rights and Privacy Act (FERPA) protected student records and electronic records that are specifically exempted from disclosure by the New York State FOIL. Private data must be protected to ensure that they are not disclosed in a FOIL request. FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy. The *NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* maps to the Category 2 - Private data risk classification.	- Final course grades - Exam questions or answers - HR employment data - Law enforcement investigation data, judicial proceedings data includes student disciplinary or judicial action information - Public Safety information - IT infrastructure data - Collective bargaining negotiation data, contract negotiation data - Trade secret data - Protected data related to research - University intellectual property - University proprietary data - Data protected by external non-disclosure agreements - Inter- or intra-agency data which are not: statistical or factual tabulations; instructions to staff that affect the public; final agency policy or determination; external audit data - University person number - Licensed software - Intellectual Property - Information created by a health care provider and used or maintained for the purposes of patient treatment, patient payment, or health care provider operations that is not regulated by HIPAA.

DATA CLASSIFICATION				
Data Risk Classification Category	**Minimum Security Standard, per National Institute of Standards and Technology**	**Risk from Disclosure**	**Definition**	**Examples**
Category 3-Public	NIST 800-53-III	Low	Includes university data not included in Category 1-Restricted and Category 2-Private, and the data is intended for public disclosure, or the loss of confidentiality of the data or system would have no adverse impact on our mission, safety, finances, or reputation. Public data includes any data that is releasable in accordance with FOIL. This category also includes general access data, such as that available on unauthenticated portions of institution's website. Public data has no requirements for confidentiality, however, systems housing the data should take reasonable measures to protect its accuracy.	- University financial data or business records available to the public - Meeting minutes - Administrative process data - Data about decisions that affect the public - Other university public data - General access data, such as that on unauthenticated portions of the institution's website

Protected Health Information (PHI)

The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. Information regulated by HIPAA may be used/maintained/disclosed within or outside of the university only as specifically permitted by the HIPAA regulations.

Background

University academic and administrative data are valuable assets and often contain detailed information about the university, as well as personal information about faculty, staff, students, and other third parties affiliated with the university. Protecting the information is driven by important considerations including legal, academic, financial, reputation, and other business requirements. This policy provides a framework for classifying university data based in its level of sensitivity, value, and criticality. Classifying data helps determine baseline security controls to protect the data.

Applicability

This policy applies to all university data and to all user-developed data sets and systems that may access these data regardless of the environment where the data reside (e.g., cloud systems, servers, personal computers, mobile devices). The policy applies regardless of the media on which data reside (e.g., electronic, printouts, CD, microfiche) or the form they may take (e.g., text, graphics, video, voice).

Data that is personal to the operator of a system and stored on a university information technology (IT) resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.

Failure to adhere to these policies and procedures may result in corrective measures. Corrective measures will be administered to a degree commensurate with the violation and in compliance with applicable collective bargaining agreements and/or applicable laws, regulations, and policies.

Definitions

Category 1- Restricted
Protection of the data is required by law/regulation. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Restricted data includes the definition of private information in the *New York State Security and Breach Notification Act* as a foundation: bank account/credit card/debit card numbers, social security numbers, state-issued driver license numbers, and state-issued non-driver identification numbers. To this list, university policy adds protected health information (PHI), computer passwords, other computer access protection data, and passport numbers.

Category 1- Restricted data are exempt from disclosure/release under the *New York State Freedom of Information Law* (FOIL). The *Information Security Breach and Notification Act* requires the university to disclose any breach of the data to New York residents. (State entities must also notify non-residents, see the *New York State Information Security Policy*.)

Individuals who access, process, store, or in any other way handle Category 1 Restricted data are required to implement controls and security measures as required by relevant laws and/or regulations in addition to any university policy. In instances where laws and/or regulations conflict with university policy, the more restrictive policy, law, or regulation should be enacted.

Category 2- Private
Includes university data not identified as Category 1- Restricted data, but includes data protected by state and federal regulations. This includes Family Educational Rights and Privacy Act (FERPA)-protected student records and electronic records that are specifically exempted from disclosure by the New York State FOIL.

Private data must be protected to ensure that they are not disclosed in a FOIL request. FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy.

The *NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* maps to the Category 2 - Private data risk classification.

Category 3- Public

Includes university data not included in Category 1- Restricted and Category 2- Private, and the data is intended for public disclosure, or the loss of confidentiality of the data or system would have no adverse impact on our mission, safety, finances, or reputation.

Public data includes any data that is releasable in accordance with FOIL. This category also includes general access data, such as that available on unauthenticated portions of institution's website. Public data has no requirements for confidentiality, however, systems housing the data should take reasonable measures to protect its accuracy.

Data Managers
University officials and their staff who have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data.

Data Owner
The University at Buffalo is considered the data owner of all university institutional data; individual units or departments may have stewardship responsibilities for portions of the data.

Data Stewards
University officials who have planning and policy-level responsibilities for data in their functional areas.

Data Trustees
Senior leaders of the university (i.e., vice presidents, vice provosts, and deans) who have responsibility for areas that have systems of record.

Data Users
Individuals who need and use university data as part of their assigned duties or in fulfillment of their role in the university community.

Responsibility

Vice President and Chief Information Officer

- Oversee the implementation of this policy.

Data Manager

- Administer activities delegated by data stewards.
- Maintain physical and system security and safeguards appropriate to the classification level of the data in their custody.

Data Steward

- Manage defined elements of institutional data.
- Implement and apply safeguards that meet or exceed the minimum safeguards for each data classification. Safeguards are determined by the individual unit, but guidance may be provided by the Information Security Office with respect to minimum expectations.

Data Trustee

- Ensure that data stewards in their area are compliant with data governance principles.

Data User

- Maintain the confidentiality, integrity, and availability of university data.
- Implement appropriate safeguards to protect data.
- Follow all university policies, procedures, and standards related to data security classification and security level, including applicable federal and state laws.

Contact Information

Office of the Vice President and Chief Information Officer
517 Capen Hall
Buffalo, NY 14260
Phone: 716-645-7979
Email: cio@buffalo.edu
Website: http://www.buffalo.edu/ubit.html

Information Security Office
201 Computing Center
Buffalo, NY 14260
Phone: 716-645-6997
Email: sec-office@buffalo.edu
Website: http://security.buffalo.edu

Related Information

University Links

Data Risk Classification Policy Appendix
Freedom of Information Law (FOIL)
Information Security: Data Access and Security Policy
Protection of University Data Policy

Related Links

Family Educational Rights and Privacy Act (FERPA) (https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html)
Freedom of Information Law (Foil) Procedures http://docs.nycenet.edu/docushare/dsweb/Get/Document-84/D-110__1-9-03.pdf

Gramm-Leach Bliley Act (https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act)

HIPAA regulated Protected Health Information (https://www.hhs.gov/answers/hipaa/what-is-phi/index.html)

New York State Freedom of Information Law (FOIL) (https://www.dos.ny.gov/coog/foil2.html)

New York State Information Security Policy (https://its.ny.gov/eiso/policies/security)

New York State Office of Information Technology Services Information Classification Standard (https://its.ny.gov/document/information-classification-standard)

New York State Security and Breach Notification Act (https://its.ny.gov/eiso/breach-notification)
NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf)

History

November 2017

Full review. Updated the policy to:

- change the title of the policy from *Data Classification Standard/Data Use Standard* to *Data Risk Classification*
- change the number of classification categories from four (i.e., Category I: Regulated Private Data; Category II: Protected Data; Category III: Internal Use Data; Category IV: Public Data) to three (i.e., Category 1 – Restricted, Category 2 – Private, Category 3 – Public); this change aligns the UB categories with the New York State Office of Information Technology Services *Information Classification Standard*
- revise data role terminology
- add HIPAA compliance reference
- provide additional data risk classification guidance including
  - FIPS 199 Security Categorization Definitions
  - Security Standard Crosswalks
  - Example Templates

DATA RISK CLASSIFICATION POLICY
APPENDICES

Appendix A: FIPS 199 Security Categorization Definitions

FIPS 199 Security Categorization Definitions			
Security Objective	**Low**	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a catastrophic adverse effect on organizational operations, organizational assets, or individuals.

Additional References:

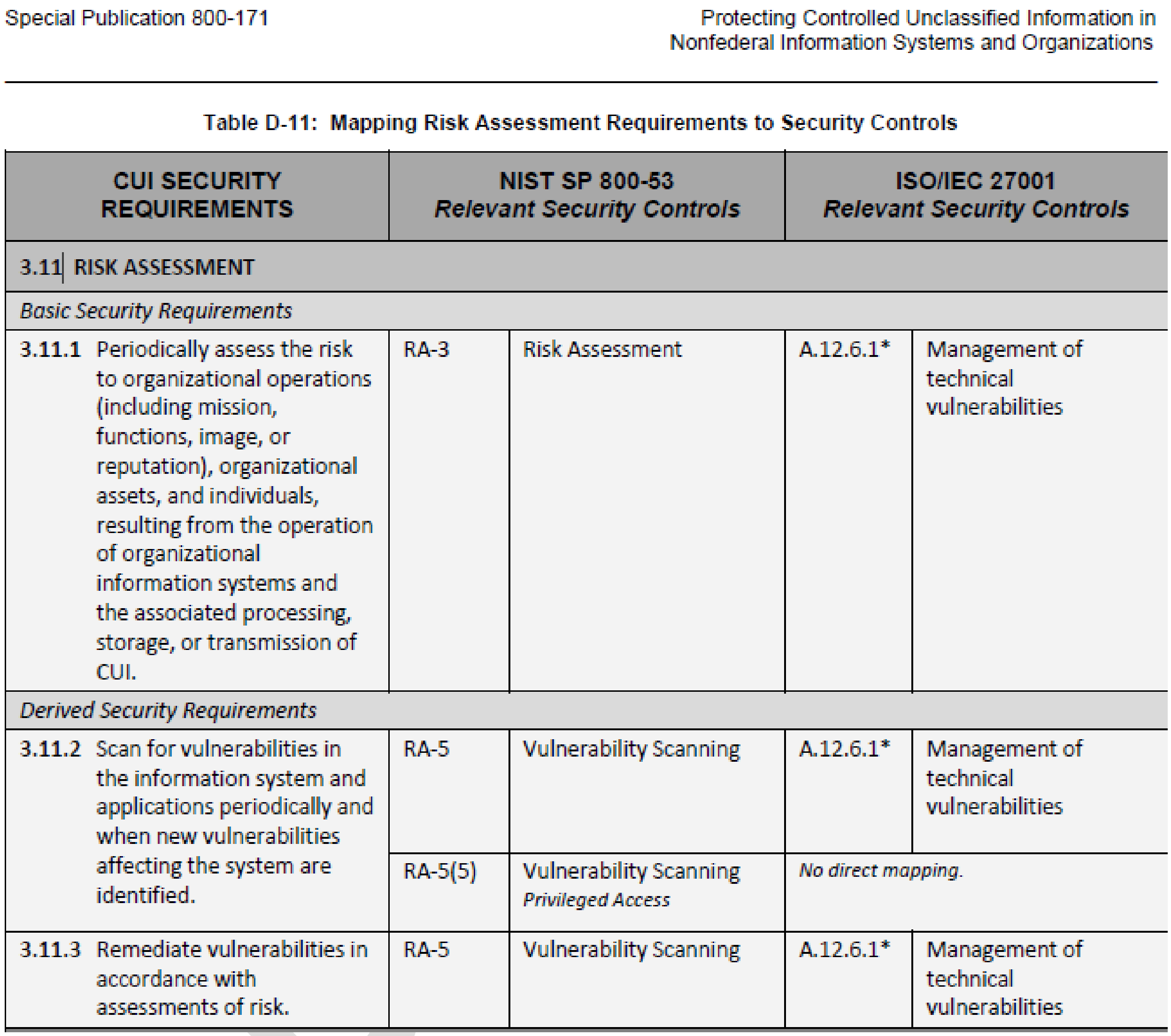
- 32 CFR Part 2002, Controlled Unclassified Information. https://www.law.cornell.edu/cfr/text/32/part-2002
- Federal Information Security Modernization Act of 2014 (P.L. 113-283), December 2014.

http://www.gpo.gov/fdsys/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

- Executive Order 13556, Controlled Unclassified Information, November 2010. http://www.gpo.gov/fdsys/pkg/FR-2010-11-09/pdf/2010-28360.pdf
- Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
- National Institute of Standards and Technology Federal Information Processing Standards Publication 199 (as amended), Standards for Security Categorization of Federal Information and Information Systems. http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- National Institute of Standards and Technology Federal Information Processing Standards Publication 200 (as amended), Minimum Security Requirements for Federal Information and Information Systems. http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
- National Institute of Standards and Technology Special Publication 800-53 (as amended), Security and Privacy Controls for Federal Information Systems and Organizations. http://dx.doi.org/10.6028/NIST.SP.800-53r4
- National Institute of Standards and Technology Special Publication 800-60 (as amended), Guide for Mapping Types of Information and Information Systems to Security Categories, Volume 1.
- http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol1-Rev1.pdf
- National Institute of Standards and Technology Special Publication 800-60 (as amended), Guide for Mapping Types of Information and Information Systems to Security Categories, Volume 2.
- http://csrc.nist.gov/publications/nistpubs/800-60-rev1/SP800-60_Vol2-Rev1.pdf 6. National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity (as amended). http://www.nist.gov/cyberframework
- Committee on National Security Systems Instruction 4009 (as amended), National Information Assurance Glossary. https://www.cnss.gov
- National Institute of Standards and Technology Special Publication 800-171
- New York State Freedom of Information Law

Appendix B: Security Standard Crosswalks

NIST Special Publication 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations



Special Publication 800-171

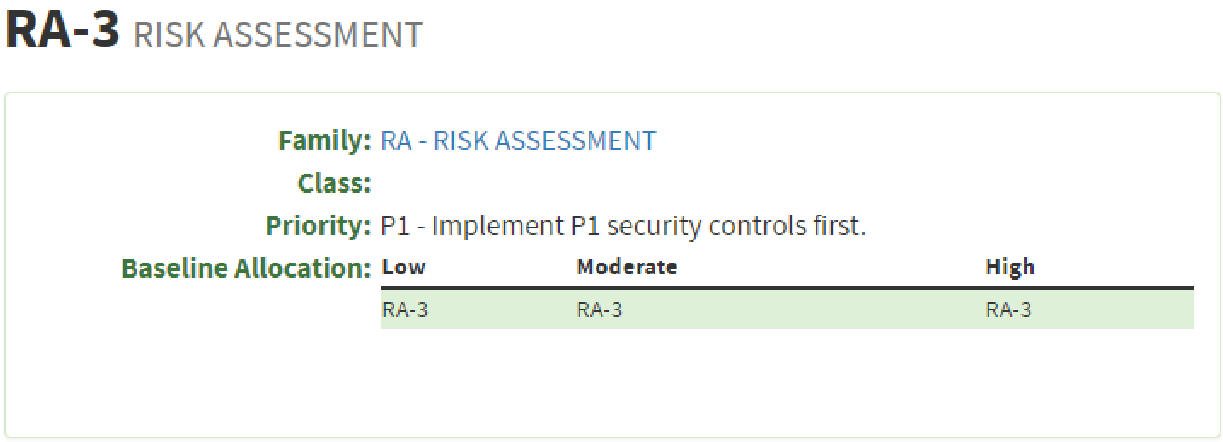
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

Table D-11: Mapping Risk Assessment Requirements to Security Controls

CUI SECURITY REQUIREMENTS	NIST SP 800-53 *Relevant Security Controls*		ISO/IEC 27001 *Relevant Security Controls*	
3.11 RISK ASSESSMENT				
Basic Security Requirements				
3.11.1 Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	RA-3	Risk Assessment	A.12.6.1*	Management of technical vulnerabilities
Derived Security Requirements				
3.11.2 Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities
	RA-5(5)	Vulnerability Scanning *Privileged Access*	*No direct mapping.*	
3.11.3 Remediate vulnerabilities in accordance with assessments of risk.	RA-5	Vulnerability Scanning	A.12.6.1*	Management of technical vulnerabilities

Source: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf

NIST Special Publication 800-53 (Rev. 4) - Security Controls and Assessment Procedures for Federal Information Systems and Organizations



RA-3 RISK ASSESSMENT

Family: RA - RISK ASSESSMENT

Class:

Priority: P1 - Implement P1 security controls first.

Baseline Allocation:

Low	Moderate	High
RA-3	RA-3	RA-3

Source: https://nvd.nist.gov/800-53/Rev4/control/RA-3

HIPAA Security Rule Crosswalk to NIST Cybersecurity - Category: Asset Management (ID.AM)

Category	Subcategory	Relevant Control mappings
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	• COBIT 5 APO03.03, APO03.04, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14 • HIPAA Security Rule 45 C.F.R. § 164.308(a)(7)(ii)(E)

Source: https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf

Additional References:
https://www.hhs.gov/sites/default/files/nist-csf-to-hipaa-security-rule-crosswalk-02-22-2016-final.pdf
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf
ISO/IEC 27001 Relevant Security Controls - A.12.6.1* Management of technical vulnerabilities

Appendix C: Example Templates

Risk Classifications: The University has classified its information assets into risk-based categories for the purpose of determining who is allowed to access the information and what security precautions must be taken to protect it against unauthorized access.

Low Risk	Moderate Risk	High Risk
Data and systems are classified as Low Risk if they are not considered to be Moderate or High Risk, and: 1. The data is intended for public disclosure, or 2. The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as Moderate Risk if they are not considered to be High Risk, and: 1. The data is not generally available to the public, or 2. The loss of confidentiality, integrity, or availability of the data or system could have a mildly adverse impact on our mission, safety, finances, or reputation.	Data and systems are classified as High Risk if: 1. Protection of the data is required by law/regulation, 2. University is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or 3. The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Data Risk Classification Examples

Use the examples below to determine which risk classification is appropriate for a particular type of data. When mixed data falls into multiple risk categories, use the highest risk classification across all.

Low Risk	Moderate Risk	High Risk
● Research data (at data owner's discretion) ● SUNet IDs ● Information authorized to be available on or through University's website without SUNet ID authentication ● Policy and procedure manuals designated by the owner as public ● Job postings ● University contact information not designated by the individual as "private" in University ● Information in the public domain ● Publicly available campus maps	● Unpublished research data (at data owner's discretion) ● Student records and admission applications ● Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information ● Non-public University policies and policy manuals ● Non-public contracts ● University internal memos and email, non-public reports, budgets, plans, financial info ● University and employee ID numbers ● Project/Task/Award (PTA) numbers ● Engineering, design, and operational information regarding University infrastructure	● Health Information, including Protected Health Information (PHI) ● Health Insurance policy ID numbers ● Social Security Numbers ● Credit card numbers ● Financial account numbers ● Export controlled information under U.S. laws ● Driver's license numbers ● Passport and visa numbers ● Donor contact information and non-public gift information

Server Risk Classification Examples

A server is defined as a host that provides a network accessible service.

Low Risk	Moderate Risk	High Risk
● Servers used for research computing purposes without involving Moderate or High Risk Data ● File server used to store published public data ● Database server containing SUNet IDs only	● Servers handling Moderate Risk Data ● Database of non-public University contracts ● File server containing non-public procedures/documentation ● Server storing student records	● Servers handling High Risk Data ● Servers managing access to other systems ● University IT and departmental email systems ● Active Directory ● DNS

Application Risk Classification Examples

An application is defined as software running on a server that is network accessible.

Low Risk	Moderate Risk	High Risk
● Applications handling Low Risk Data ● Online maps ● University online catalog displaying academic course descriptions ● Bus schedules	● Applications handling Moderate Risk Data ● Human Resources application that stores salary information ● Directory containing phone numbers, email addresses, and titles ● University application that distributes information in the event of a campus emergency ● Online application for student admissions	● Applications handling High Risk Data ● Human Resources application that stores employee SSNs ● Application that stores campus network node information ● Application collecting personal information of donor, alumnus, or other individual ● Application that processes credit card payments

Approved Services Example Template: This table indicates which classifications of data are allowed on a selection of commonly used approved university IT services.

Service	Low Risk	Moderate Risk	High Risk: Non-PHI[1]	High Risk: PHI
Audio and Video Conferencing:	✓	✓	✓	✓
Infrastructure	✓	✓	✓	
Backups:	✓	✓	✓	✓
Content Management:	✓	✓		
Content Management:	✓	✓		
Calendar:	✓	✓		
Database Hosting:	✓	✓		
Document Management:	✓	✓	*	
Document Management:	✓	✓	✓	✓
Document Management:	✓	✓	*	
Document Management:	✓	✓	*	
Email:	✓	✓		
Email:	✓	✓		
Email:	✓	✓	✓	✓
Email:	✓	✓		
Encryption:	✓	✓	✓	✓
Encryption:	✓	✓	✓	✓
Encryption:	✓	✓		
File Storage:	✓	✓		
File Storage:	✓	✓	✓	✓
File Storage:	✓	✓		

Service	Low Risk	Moderate Risk	High Risk: Non- PHI[1]	High Risk: PHI
File Storage:	✓	✓	✓	✓
File Transfer:	✓	✓	✓	✓
Form Builder:	✓	✓		
Google	✓	✓		
Instant Messaging:	✓	✓	✓	✓
Issue Tracking:	✓	✓		
Microsoft Azure	✓	✓		
Network Access Control:	✓	✓	✓	✓
Request Tracking:	✓	✓		
Shared Computing:	✓	✓		
University Profiles:	✓			
Survey Tool:	✓	✓		✓
Voice Messaging	✓	✓		
VPN	✓	✓	✓	✓
Web Programming:	✓	✓		
Wiki: Confluence	✓	✓		

[1] Payment Card Industry (PCI) data has special regulatory requirements that preclude using the services above. Contact the PCI team for assistance with handling this type of data.

* High Risk Data not currently permitted, pending Data Loss Prevention (DLP) solution deployment.

Source: Stanford University