University System of New Hampshire

SECURITY CATEGORIZATION STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: PUBLIC
Status: IN FORCE

1 PURPOSE

This Standard defines the process for determining the Security Categorization of information technology resources and critical business processes at the University System of New Hampshire (USNH).

Security Categorization is a risk management designation used across the Cybersecurity Program to consistently express the criticality of an information technology resource or business process. This designation is based on the institutional information involved and the breadth of impact if that resource or process were compromised.

A security category is a short-hand designation that conveys the importance of securing a specific information technology resource or business process. By allocating resources and processes into common and standardized categories, we are better able to match security controls appropriately to the resources/processes, and we are also better able to prioritize security activities and risk management investments.

Unlike the factors used in the risk analysis process, which are used to quantify specific risks, security categories relate only to the information technology resource or business process, and do not change based on threat events or vulnerabilities.

2 SCOPE

This Standard applies to all USNH information technology resources that capture, store, process, transmit, or otherwise manage institutional information, regardless of that information's classification. Additionally, this Standard applies to any administrative, academic, or business unit process that is designated as a "critical business process" for cybersecurity risk management purposes as defined in the *Cybersecurity Risk Management Standard*.

University System of New Hampshire

3 AUDIENCE

All USNH community members who are responsible for management or administration of information technology resources and those community members who participate in or manage administrative, academic, or business unit processes that are in-scope for this Standard should understand this Standard and how it might impact their responsibilities.

4 STANDARD

OVERVIEW

Enterprise Technology & Services (ET&S) Security Categorization follows the structure established in FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems.*

Security categories are assigned to specific assets, like information technology resources, or to specific business processes, as the basis for determining the potential impact of a cybersecurity event on that specific asset or process. The ET&S Security Categorization process is based on three factors:

- The classification, per the *USNH Information Classification Policy*, of the institutional information used in the business process or that is captured, stored, processed, transmitted, or otherwise managed by the information technology resource
- The magnitude of the impact if that information were compromised
- Whether the impact involves a loss of confidentiality, integrity, or availability

Security Categorization is used in a variety of ways, including but not limited to:

- Determining the security control baseline for a specific information technology resource or business process
- Informing loss magnitude determination as part of the Cybersecurity Risk Assessment process
- Contributing to the risk assessment of cybersecurity exception requests

The Chief Information Security Officer (CISO) is responsible for the Security Categorization process.

INFORMATION TYPE DETERMINATION

All ET&S Security Categories are based on information types which are defined using two factors.

The first factor is the Information Classification Tier, per the *USNH Information Classification Policy*, of the information involved in the business process or used by the information technology resource. The current USNH Information Classifications are:

- Tier 1 – Public
- Tier 2 – Sensitive

- Tier 3 – Protected
- Tier 4 – Restricted
- Tier 5 – Confidential

Definitions and examples of each classification are available in the *USNH Information Classification Policy*.

The second factor is the breadth of the information. This is determined based on the number of USNH institutions whose information could be impacted. There two levels used to define breadth – USNH and Institution.

- USNH: Used when the information that could be impacted includes data from two or more component institutions. Examples of information sets that would be assigned a USNH factor include:
    - The Banner HR/Finance Environment which contains information about all USNH employees
    - A student success application that pulls information from each of the institutional Student Information Systems and therefore contains information about all USNH students
    - A business process that involves handling employee PII for all USNH institutions
- Institution: Used when the information that could be impacted includes data from only one USNH Institution. Examples of information sets that would be assigned the Institution factor:
    - ePHI used by an institution's Student Health Center
    - Financial Aid data used by an institution's financial aid office to process financial aid application for that institution's students

The combination of these two factors results in the following USNH Information Types:

- Public – USNH
- Public – Institution
- Sensitive – USNH
- Sensitive – Institution
- Protected – USNH
- Protected – Institution
- Restricted – USNH
- Restricted – Institution
- Confidential – USNH
- Confidential - Institution

POTENTIAL IMPACT DETERMINATION

In line with the process outlined in FIPS 199, ET&S uses the following levels to define the potential impact of an adverse cybersecurity event that compromises confidentiality, integrity, and/or availability.

Impact = MINIMAL

The security category is minimal if a loss of confidentiality, integrity, or availability could result in a very limited adverse effect on one or more administrative, academic, or business units, with no real impact at the component institution level.

Examples: Loss of confidentiality, integrity, or availability that results in:

- Minimal impact to budget or finances, financial impact can be recovered at the unit level in the current year's budget without a budget/financial variance
- Minimal damage to or loss of information technology resources like endpoint computers, can be recovered at the unit level without impacting current year budget
- No discernible impact to achievement of administrative, academic, or business unit objectives
- No impact to reputation or enrollment
- No impact to life and safety

Impact = MODERATE

The security category is moderate if a loss of confidentiality, integrity, or availability could result in minor adverse effects on one or more administrative, academic, or business units, with no real impact at the component institution level.

Examples: Loss of confidentiality, integrity, or availability that results in:

- Minor impact on budget or finances:
    - Financial impact can be recovered in the current year's budget but may require a small budget variance
    - Can be handled internally, without requiring assistance at the component institution level
- Minor damage to or loss of information technology resources like endpoints or servers, can be replaced or recovered within the current year's budget
- Minimal impact to ability of an administrative, academic, or business unit to achieve one or more of its objectives, but does not have a discernible impact on achievement of overall mission and does not impact the component institution’s ability to achieve its objectives
- Limited potential for impact to reputation or enrollment (e.g., local news coverage for a single news cycle)
- No impact to life and safety

Impact = SIGNIFICANT

The security category is significant if a loss of confidentiality, integrity, or availability could result in significant adverse effects on one or more administrative, academic, or business units, as well as the potential for discernible impacts at the component institution level.

Examples: Loss of confidentiality, integrity, or availability that results in:

- Significant impact on budget or finances
    - Financial losses may be recoverable within current year, but will require reprioritization of funds within internal budget
    - Financial losses may require a budget variance that needs assistance or approval at the component institution level
- Significant damage to or loss of information technology resources that cannot be recovered in the current fiscal year by the impacted unit, requires assistance at the component institution level
- Significant impact to ability of an administrative, academic, or business unit to achieve its mission, potential for a discernible impact on achievement of the component institution's objectives
- Discernible impact to reputation with potential for a discernible impact to enrollment (e.g., persistent local news coverage lasting longer than a week, numerous calls/complaints to component institution leadership)
- Potential for minimal harm to individuals due to losses that impact life and safety systems or processes

Impact = MAJOR

The security category is major if a loss of confidentiality, integrity, or availability could result in substantial adverse effects on several administrative, academic, or business units and at the at the component institution level.

Examples: Loss of confidentiality, integrity, or availability that results in:

- Substantial impact to budget/finances
    - Substantial losses that are not recoverable within the current fiscal year at the institutional level, requires assistance at the system level
    - Requires budget variance for current and next fiscal year
- Substantial damage to or loss of information technology resources, cannot be recovered in the current fiscal year by the impacted institution, requires assistance at the system level
- Substantial impact to ability of an administrative, academic, or business unit AND impacted institution(s) to achieve objectives and overall mission
- Major impact to reputation with expected discernible impact on enrollment or hiring (e.g., national news coverage)
- Actual harm to individuals due to loss impacting life and safety systems or processes that includes life threatening injuries or loss of life or resulting from a data loss that leads to real-world safety concerns

Impact = CATASTROPHIC

The security category is catastrophic if a loss of confidentiality, integrity, or availability could result in unacceptable adverse effects on several component institutions and at the University System level:

Examples: Loss of confidentiality, integrity, or availability that results in:

- Severe impact to budget/finances:
  - Unacceptable financial losses that cannot be recovered in this or the next fiscal year
  - Endangers financial sustainability of one or more component institutions
- Severe damage to or loss of information technology resources, restoration requires diversion of funds at the system level
- Severe impact to institution(s) ability to achieve mission, potentially institution-ending impact
- Catastrophic impact to reputation with expected significant impact on enrollment and hiring (e.g., Persistent national news coverage)
- Grave harm to individuals due to loss impacting life and safety systems or processes that includes life threatening injuries and loss of life

SECURITY CATEGORIZATION OF INFORMATION TYPES

Per the FIPS 199 process, in order to determine the appropriate security categorization of an information type, the potential impact for all three security objectives shall be assessed. ET&S uses the formula provided in FIPS 199 to make this determination.

"Security Category (SC): "Information Type" = (Confidentiality, "Impact") (Integrity, "Impact") (Availability, "Impact")"

Using this formula, all USNH Information Types were assessed and assigned impact scores for each security objective. In determining which categorization is appropriate, it was assumed that all institutional information available to be adversely impacted within each information type, would be adversely impacted. For example, if there was a loss of confidentiality for the Protected – USNH information type, the categorization assumes that all student records for all students at all institutions would be impacted.

The resulting Security Categorization for each Information Type is provided below.

Information Type	Confidentiality Impact	Integrity Impact	Availability Impact	Security Category
Public – Institution	MINIMUM	MINIMUM	MINIMUM	**MINIMUM**
Public – USNH	MINIMUM	MINIMUM	MINIMUM	**MINIMUM**
Sensitive – Institution	MODERATE	MODERATE	MODERATE	**MODERATE**
Sensitive – USNH	MODERATE	MODERATE	MODERATE	**MODERATE**
Protected – Institution	SIGNIFICANT	SIGNIFICANT	SIGNIFICANT	**SIGNIFICANT**
Protected – USNH	MAJOR	MAJOR	MAJOR	**MAJOR**
Restricted – Institution	SIGNIFICANT	SIGNIFICANT	SIGNIFICANT	**SIGNIFICANT**

Restricted – USNH	CATASTROPHIC	MAJOR	MAJOR	**CATASTROPHIC**
Confidential – Institution	CATASTROPHIC	CATASTROPHIC	CATASTROPHIC	**CATASTROPHIC**
Confidential - USNH	CATASTROPHIC	CATASTROPHIC	CATASTROPHIC	**CATASTROPHIC**

As indicated in the chart above, when the three impact designations are not the same, the highest category applies. This means that a Security Category of MIN can only be assigned when all three security objective impacts are MINIMUM and a CATASTROPHIC in any of the security objective impacts always results in a Security Category of CATASTROPHIC.

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the *USNH Cybersecurity Policy*, the processes and procedures that support the requirements defined in this Standard shall be reviewed, and where needed, updated to ensure currency and continuous improvement.

6 ENFORCEMENT

Failure to comply with this Standard puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures shall be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., Student Rights, Rules, and Responsibilities).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

7 EXCEPTIONS

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the *Cybersecurity Exception Standard*.

University System of New Hampshire

8 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Units:

- Determine the Security Categorization of all information technology resources, and business processes used within the unit, with the assistance of Cybersecurity GRC
- Sign-off on security categorizations for information technology resources and critical business processes

Chief Information Security Officer (CISO):

- Review and revise the impact designations for each Information Type
- Sign-off on all security categorizations

Cybersecurity Governance, Risk, and Compliance (GRC):

- Maintain all documentation related to the Security Categorization process
- Assist administrative, academic, and business units in understanding the Security Categorization of their business processes and information technology resources
- Conduct a review and confirmation of established security categorizations as part of the Risk Assessment Process
- Maintain a list of all current security categorizations

Technology Service Owners:

- Determine the Security Categorization of all information technology resources, and business processes used within the unit, with the assistance of Cybersecurity GRC
- Sign-off on security categorizations for information technology resources and critical business processes

9 DEFINITIONS

See the ET&S Policy & Standard Glossary for full definitions of each term.

- Asset
- Availability
- CONFIDENTIAL Information
- Confidentiality
- Critical Business Process
- Exception
- Information
- Cybersecurity Event
- Information Technology Resource

University System of New Hampshire

- Institutional Information
- Integrity
- PROTECTED Information
- PUBLIC Information
- RESTRICTED Information
- Risk
- Risk Acceptance
- Risk Assessment
- Security Categorization
- Security Control
- SENSITIVE Information
- Technology Service Owner

10 Related Policies and Standards

- USNH Information Classification Policy
- USNH Cybersecurity Policy
- Cybersecurity Exception Standard
- Cybersecurity Risk Acceptance Standard
- Cybersecurity Risk Management Standard
- Security Configuration Management Standard
- Vulnerability Management Standard

CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

DOCUMENT HISTORY

Effective Date:	15 FEB 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 27 JAN 2021 V1

University System of New Hampshire

	CYBERSECURITY POLICY & STANDARD WORKING GROUP, 27 AUG 2020 v0.3
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, JAN 2021 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, AUG 2020
Revision History:	REVISED PER CS P&S WORKING GROUP, AUG 2020 REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 09 MAR 2020