MINNESOTA STATE

Chapter 5 – Administration
Operating Instruction

Operating Instruction 5.23.3.1 Information Security Controls

Part 1. Purpose
To establish the framework for identifying an appropriate and consistent set of information security controls for Minnesota State Information technology systems (IT Systems) to be used to meet information security requirements as set forth in System Procedure 5.23.3 Information Security Requirements and Controls.

Part 2. Applicability
These operating instructions apply to any IT system used by a Minnesota State institution, whether the IT system is owned or hosted by the system office, a campus, or a third party.

These operating instructions and related Non-functional requirements (NFRs) are to be used by the architects and implementers of IT systems to ensure that when IT systems are purchased or implemented, an appropriate and consistent set of information security controls are applied to the IT system.

Nothing in these operating instructions shall be interpreted to expand, diminish, or alter the academic freedom provided under board policy, a collective bargaining agreement, the terms of any charter establishing a system library as a community or public library, or Board Policy 5.22 Acceptable Use of Computers and Information Technology Resources.

Part 3. Definitions
For purposes of these operating instructions, the following definitions apply:

Assurance profile
A list of Non-functional Requirements for the protection of data confidentiality (C) and data integrity (I). An Assurance Profile for both C and I are derived from responses to the Information Security Controls Interview Questionnaire. Assurance profiles are defined as: Minimum, Low, Medium, or High.

Data custodian
The data custodian is appointed by the data owner to assign the security classifications for institutional data and ensuring the appropriate controls are implemented.

Data owner

An individual with ultimate authority and accountability for specified information (e.g., a specific business function) or type of institutional data. Included in this authority is the ability to grant and deny access to data or portions of institutional data under his or her control. This individual is responsible for delegating responsibility to appropriate data custodians to ensure the protection of data confidentiality of institutional data. The data owner is typically an individual in a business or academic senior or high-level leadership position. There may be more than one data owner at a college, university or system office depending on the authority and accountability for specified information (e.g., a specific business function) or type of institutional data.

Information security controls

Technical, administrative, management, or physical methods or safeguards that, when applied satisfy information security requirements. For example, an information security requirement may state, "confidential data in transit over a public network (i.e., Internet) must be unreadable to any unauthorized individual." The information security control for meeting this requirement could be to apply encryption to any confidential data when it is transmitted over the Internet.

Information security requirements

Information security obligations that must be met or implemented. Information security requirements are defined by, for example, federal or state law or regulation, industry regulations, state statute, board policy or procedures, third-party contracts, college or university policy, or any other information security protection requirement identified by the data owner.

Information technology service provider

An internal or external entity that provides or manages an Information Technology system.

Information technology system (IT system)

Any computer, server, software application, networking infrastructure, storage device, or medium, etc., that provides for information processing, transfer, storage, or communications.

Institutional data

Data collected, manipulated, stored, reported, or presented in any format, on any medium, by any unit of the college, university, or system office that are created, received, or maintained by the institution for Minnesota State.

Non-functional requirements (NFRs)

Requirements other than those that specify business or application functionality (functional requirements). Non-functional requirements describe how well an IT system does whatever it does and under what constraints the IT system must operate. NFRs describe operational characteristics, performance, information security requirements, etc.

Non public data
Any data classified by statute, federal law, or temporary classification as confidential, private, nonpublic, or protected nonpublic as defined in the Minnesota Government Data Practices Act (MGDPA) or equivalent classification in any other relevant state or federal statute.

System information technology
All system facilities, technologies, and information resources used for information processing, transfer, storage, and communications. This includes, but is not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management IT systems; and computing and electronic communications devices and services, such as modems, e-mail, networks, telephones, voicemail, facsimile transmissions, video, mobile computing devices, and multimedia materials.

Part 4. Operating Instructions

These operating instructions define the framework and process for identifying non-functional requirements (NFRs) for an IT system. Non-functional requirements define the information security controls that must be implemented for the IT system.

A tool is available that can be used to identify NFRs for an IT system (see *ESG Evaluation Tool* in the Related Documents section at the end of these operating instructions). The tool is designed to reduce the amount of manual steps to identify NFRs. Using the tool is a two-step process:

1. **Answer the questions in the 'questionnaire' tab – These questions can also be found in Subpart A of these operating instructions**
2. **Click on the 'generate report' button at the bottom of the questionnaire**

The output is a report that lists the NFRs that apply to the IT system being evaluated

These operating instructions are structured as follows:

- **Part 4. Subpart A. Information security controls - interview questionnaire**. This subpart contains the questionnaire that must be completed by the data owner and/or IT staff to identify the sensitivity of the data and the characteristics of the IT system.

- **Part 4. Subpart B. Mapping tables**. The four mapping tables in this section define a mapping from IT system characteristics as specified in the interview questionnaire to required levels of protection of data confidentiality (C) and data integrity (I), termed as 'assurance profiles.' After completing all of the mapping tables, the most stringent assurance profile identified for each objective – data confidentiality (C) and data integrity (I) – is used in the remaining parts of these operating instructions.

- **Part 5. Assurance profiles**. Each of the confidentiality and integrity assurance profiles are defined in this section, including the specific non-functional requirements (NFRs) that must be met or implemented.

- **Appendices A – H**. These appendices are all the applicable NFRs including the category (e.g., security or recoverability), the goal of the NFR, the rationale, and the metric to which the information security control must be implemented.

Subpart A. Information security controls - interview questionnaire
The process for determining the appropriate information security controls that apply to an IT system begins with this questionnaire that is to be completed by the IT system's data owner and/or IT staff (i.e., stakeholders). Answers to the questions will be used to apply the information security controls framework to identify the applicable NFRs.

Questionnaire
The following questions are to be answered to identify the following:

- IT system purpose, business, or academic function
- The IT system data owner or department that would be considered the owner
- The type and criticality of the data that the IT system stores or transports
- Characteristics of the IT system including:
    - From where the IT system can be accessed – i.e., Internet, internal only, etc.
    - The relationship between the owner of the IT system, the custodian of the data, and the provider of the IT system/service
    - Whether it is an IT system of record or a copy from another source
    - The number of individuals that would be adversely affected by a failure of data confidentiality or data integrity of the IT system

IT system purpose and data owner questions:

1. What is (are) the purpose(s) of the IT system – i.e., business or academic function the IT system serves?
   Explain: ____________________________
2. Who is the data owner of the IT system or the logical department that it serves that could be considered the owner?
   IT system data owner or department name: _________________________

Data confidentiality and integrity – Typically answered by the IT system data owner

Place an 'X' in the right-hand column if applicable

Confidentiality	
The IT system stores or transfers highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	
The IT system stores or transfers Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	
The IT system stores or transfers Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	

Integrity	
The IT system stores or transfers official academic records (e.g., student transcripts, grades) or financial data that could affect the financial position of the organization (e.g., system office or a college's/university's bank account information)	
The IT system stores or transfers data used to make any financial, academic or personnel decisions	
The IT system stores or transfers informational data only	

System Characteristics – IT system data owner and/or IT staff questions

Note: The IT system data owner may be positioned best to answer questions under *user impact* and *system of record*. The IT department may be positioned best to answer the questions under *IT system exposure* and *owner / custodian / IT service provider*.

Place an 'X' in the cell below the statement if applicable

User Impact
<u>Description:</u> *The framework asserts that a failure of either data confidentiality or data integrity of an IT system will be roughly proportional to the number of affected persons. The framework asserts that a failure affecting a large number of people will have a greater impact on Minnesota State than the same failure affecting a small number of persons. In general, the user impact characteristic will have a significant impact on requirements in both areas (C and I).* *As applied to this framework, 'users' should be counted as:* • *Confidentiality: The number of individuals adversely affected by a failure of confidentiality of the IT system.* • *Integrity: The number of individuals adversely affected by a failure of integrity of the data stored or managed by the IT system.*

<table>
<tr><td colspan="4"></td></tr>
<tr><td>The IT system contains, or is expected to contain, fewer than 250 individuals’ not public information</td><td>The IT system contains, or is expected to contain, 250 – 24,999 individuals’ not public information</td><td>The IT system contains, or is expected to contain, 25,000 – 249,999 individuals’ not public information</td><td>The IT system contains, or is expected to contain, more than 250,000 individuals’ not public information</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="3">IT System Exposure</th></tr>
<tr><td colspan="3"><u><i>Description:</i></u>
<i>The IT system exposure characteristic is intended to guide implementers toward a higher level of confidentiality and integrity requirements on IT systems that are exposed to the Internet, and permit IT systems that are well sheltered from public, guest or other uncontrolled networks to be implemented with fewer requirements.</i></td></tr>
<tr><td>The IT system is only accessible from internal business network(s) on campus or at the system office</td><td>The IT system is only accessible from the Minnesota State wide area network, system office, or campus network(s)</td><td>The IT system is accessible from the Internet or publically accessible unauthenticated networks</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="3">System of Record</th></tr>
<tr><td colspan="3"><u><i>Description:</i></u>
<i>The intended outcome is that IT systems which are the system of record for data that will either affect the organization financially or that will be used by the organization to make decisions, are protected with a reasonable set of integrity-related requirements. The System of Record characteristic is expected to have the greatest impact on the integrity-related requirements. Systems that have downstream dependencies must have somewhat greater protection against integrity incidents, while IT systems that are easily re-creatable can have somewhat lesser integrity requirements.</i></td></tr>
<tr><td>The data contained in the IT system is a copy of data from another source</td><td>The IT system is a system of record but there are <i>no other</i> IT systems, business, or academic processes that are dependent on it for correct and accurate data</td><td>The IT system is a system of record with data that cannot be replaced; and other IT systems, business, or academic processes are dependent upon it for accurate information</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

<table>
<tr><th colspan="3">Owner / Custodian / IT Service Provider</th></tr>
<tr><td colspan="3"><em>Description:</em>
<em>The owner-custodianship characteristic is intended to require a higher level of controls on IT systems that are outsourced, either to other institutions within Minnesota State or to non-Minnesota State IT Service Providers. The owner-custodianship characteristic is structured to permit greater flexibility on requirements for IT systems that do not span organizational boundaries.</em></td></tr>
<tr><td>The owner, custodian, and IT service provider are part of the same college, university, or the system office.</td><td>The custodian or IT service provider is not in the same college, university, or the system office as the owner.</td><td>Either the custodian or the IT Service Provider is a non-Minnesota State entity (e.g., cloud provider).</td></tr>
</table>

Subpart B. Mapping Tables

The four Mapping Tables below are structured as follows:

- The impact rating for confidentiality and integrity is defined in the left-hand column. The content in this column does not change in any of the four mapping tables
- IT system characteristics are defined in the column headings of the mapping table. Each of the four mapping tables defines a different IT system characteristic with different levels or variables of the characteristic
- The body of the table under the IT system characteristic is the assurance profiles for confidentiality (C) or integrity (I). assurance profiles range from Minimum to high for both confidentiality and integrity (e.g., C-Minimum, C-Low, C-Medium, C-High, I-Minimum, I-Low, I-Medium, I-High)

Steps

Based on the answers provided in Subpart A, follow the six (6) steps below to identify the appropriate C and I assurance profiles. The assurance profiles, found in Part 5, define the appropriate NFRs that apply to the IT system.

1) Using the responses from the data confidentiality and integrity section of the information security controls - interview questionnaire, determine the impact rating for confidentiality (C) and integrity (I) identify the impact rating in the first column. This impact rating will be applied to each of the four IT system characteristic mapping tables.
2) Using the responses to the IT system characteristics section of the information security controls - interview questionnaire, identify the column heading in the appropriate characteristic mapping table that matches the response.
3) In each of the characteristic mapping tables, use the C and I impact rating and the IT system characteristic response to determine the assurance profiles for both C and I of the mapping table. The C and I assurance profiles are identified in the cell where the impact rating and characteristic response intersect.
4) Identify the highest assurance profile for both C and I from all of the IT system characteristics mapping tables. The results are a 'confidentiality assurance profile' and an 'integrity assurance profile.'
5) Using the highest assurance profiles identified in step 4, reference Part 5 assurance profiles, to determine the appropriate NFRs that must be implemented as information security controls for the IT system.
6) Implement information security controls identified in Step 5.

If the impact rating for C or I changes, or characteristics of an IT system change such that it would render a different response to a question in the information security controls - interview questionnaire, the IT system must be reevaluated by completing the 6 steps above and re-implement controls.

Subpart B.1. User Impact Mapping Table

	User Impact			
Impact Rating	Low number of individuals' not public information (<250)	Medium number of individuals' not public information (250 – 24,999)	High number of individuals' not public information (25,000 – 249,999)	Very high number of individuals' not public information (>250,000)
Confidentiality:				
Highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Low**	**C-Medium**	**C-Medium**	**C-High**
Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Low**	**C-Medium**	**C-Medium**
Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Minimum**	**C-Minimum**	**C-Minimum**
Integrity:				
Data that affects the financial position of the organization or IT systems that contain official academic records	**I-Low**	**I-Medium**	**I-Medium**	**I-High**
Used to make financial, academic, or personnel decisions	**I-Low**	**I-Low**	**I-Low**	**I-Medium**
Informational only	**I-Minimum**	**I-Minimum**	**I-Minimum**	**I-Minimum**

Subpart B.2. IT system Exposure Mapping Table

	IT system Exposure		
Impact Rating	Limited to internal business networks	Accessible only from the Minnesota State wide area network, system office, or campus network(s)	Accessible from Internet (and/or guest, public, Internet)
Confidentiality			
Highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Low**	**C-Low**	**C-Medium**
Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Low**	**C-Medium**
Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Minimum**	**C-Minimum**
Integrity:			
Data that affects the financial position of the organization or IT systems that contain official academic records	**I-Low**	**I-Low**	**I-Medium**
Used to make financial, academic, or personnel decisions	**I-Low**	**I-Low**	**I-Low**
Informational only	**I-Minimum**	**I-Minimum**	**I-Minimum**

Subpart B.3. System of Record Mapping Table

	System of Record		
Impact Rating	Downstream copy, re-creatable via replication	System of record, no dependent IT systems	System of record, with dependent IT systems
Confidentiality			
Highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Low**	**C-Low**	**C-Medium**
Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Low**	**C-Low**
Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Minimum**	**C-Minimum**
Integrity:			
Data that affect the financial position of the organization or IT systems that contain official academic records	**I-Low**	**I-Medium**	**I-High**
Used to make financial, academic, or personnel decisions	**I-Low**	**I-Low**	**I-Low**
Informational only	**I-Minimum**	**I-Minimum**	**I-Minimum**

Subpart B.4. Owner/Custodian/IT Service Provider Mapping Table

Impact Rating	Ownership/Custodianship/IT Service Provider		
	The owner, custodian, and IT service provider are part of the same college, university, or system office	The custodian or IT service provider are not in the same college, university, or system office as the owner	Either the custodian or the IT service provider is a non-Minnesota State entity (e.g., cloud provider)
Confidentiality			
Highly restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Low**	**C-Low**	**C-Medium**
Restricted data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Low**	**C-Medium**
Low data as defined in System Procedure 5.23.2 Data Security Classification and Operating Instructions 5.23.2.1 Data Security Classification	**C-Minimum**	**C-Minimum**	**C-Minimum**
Integrity:			
Data that affects the financial position of the organization or IT systems that contain official academic records	**I-Low**	**I-Low**	**I-Medium**
Used to make financial, academic, or personnel decisions	**I-Low**	**I-Low**	**I-Low**
Informational only	**I-Minimum**	**I-Minimum**	**I-Minimum**

Part 5. Assurance Profiles

Assurance profiles are structured as follows:

- Subparts A-H in this section are the eight (8) data confidentiality and data integrity assurance profiles – e.g., C-Minimum through C-High and I-Minimum through I-High.
- The NFRs within each assurance profile define the category (security or recoverability) followed by the requirement metrics (i.e., bullets).

Notes: The complete detailed NFRs and the metrics can be found in Appendices A–H. NFR metrics define required outcomes versus prescriptive technical implementation requirements.

Subpart A. Data confidentiality minimum (C-Minimum)

NFR - security - configuration integrity

- **D1** - The recovered IT system will meet all pre-modification functional and non-functional requirements
- **D2** - The IT system will meet Operating Instructions 5.23.1.8 Anti-malware Installation and Management
- **D3** - A process exists that meets Operating Instructions 5.23.1.4 Information Security Incident Response
- **D4** - IT systems preforming storage, business logic, or unencrypted transmission of data classified as highly restricted or restricted must be administered by personnel using least privilege

NFR – security - configuration assessment

- **D1** - The configuration of the IT system will meet a documented standard or benchmark
- **D2** - The IT system patch intervals will meet requirements in Operating Instructions 5.23.1.5 Security Patch Management

NFR – security - data access

- **D1** - A process for granting and revoking logical and physical access is implemented
- **D2** - Credentials used to access the IT system or data meet controls and guidance defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3
- **D3** - Logical and physical security perimeters are identified and documented
- **D4** - The IT systems storing or managing the data will have network segmentation controls implemented to meet controls and guidance defined in ISO 27002, section 13.1.3

NFR – security - data classification

- **D1** - The data managed by the IT system has an assigned owner
- **D2** - The data managed by the IT system has been classified as highly restricted, restricted, or low

NFR – security - data encryption

- **D2** - Logical and physical security perimeters are identified and documented
- **D3** - Data classified as highly restricted or restricted stored, transported, or transmitted to a higher risk network or perimeter is encrypted

NFR – Security - awareness and training

- **D1** - IT system administrator(s) must complete Public Jobs: Private Data courses: *Data Security in Your Job, Securing Your Computer Workstation and Using Data in the Workplace*

Subpart B. Data Confidentiality Low (C-Low)

Include all of *data confidentiality minimum,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum, or it may be a new requirement:

NFR - Security - configuration assessment

- **C1** - The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than 90 days
- **C2** - An automated, systematic means of mitigating software vulnerabilities must exist.
- **C3** - The configuration of the IT system will meet a current vendor-provided standard or benchmark
- **C4** - Modification of IT system configuration is restricted to individuals that meet security - awareness and training non-functional requirement

NFR - Security - data access

- **C1** - IT system administrator and user access is logged
- **C2** - Individual access to the IT system and data is reviewed annually
- **C3** - Unique credentials are required for each individual accessing the data
- **C4** - A documented relationship exists between data owner and data custodian
- **C5** - Logical controls exist that enforce a default deny policy from lower to higher security perimeters

NFR – Security - data encryption

- **B1** - Credentials, other than UserID, for accounts with privileges sufficient to modify IT system configuration are encrypted when stored or transmitted

NFR – Security - awareness and training

- **C1** - IT system administrator(s) must be offered at least forty hours of job related formal training per year

- **C2** - IT system administrator(s) must annually complete Public Jobs: Private Data courses: *Data Security in Your Job*; *Securing Your Computer Workstation and Using Data in the Workplace*; *Data Security for Faculty, Managers and Supervisors*;

Managing Student Data Securely; *Managing Financial Data Securely*; and *Managing Personnel Data Securely*

Subpart C. Data confidentiality medium (C-Medium)

Include all of *Data Confidentiality Minimum and Low,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum or low, or it may be a new requirement:

NFR – Security - configuration integrity

- **B1** - A non-refutable log of all access and modifications to the IT system configuration by accounts with privileges sufficient to modify IT system configuration will exist and contain action performed, individual, IP address, date and time for a period of one year
- **B2** - No more than one business day of IT system modifications will be lost
- **B3** - Access and modification of IT system configuration will be conducted using privileges limited to the minimum required to complete the activity

NFR – Security - configuration assessment

- **B1** - The configuration of the IT system will be verified by automated rule based systems at intervals no longer than 30 days
- **B2** - The configuration of the IT system will be compared against Center for Internet Security (CIS) level 1 or equivalent and differences documented
- **B3** - A formal process exists for assessing configuration modifications prior to implementation

NFR – Security - data access

- **B1** - The IT system will maintain a non-refutable log of all access and modifications to highly restricted IT system managed data sufficient to determine the individual, IP address, date, and time
- **B2** - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration
- **B3** - Tools and processes exist that detect, log, and alert on unauthorized access to the IT system and to data managed by the IT system
- **B4** - When work assignments change, access is updated to reflect new work assignment
- **B5** - Access to data is based on assigned roles
- **B6** - Documented business or functional requirements identify the privileges required to perform all business functions that access or modify highly restricted or restricted data
- **B7** - System accounts will conform to meet requirements defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3

NFR – Security - data encryption

- **A2** - Key recovery for symmetric keys will be implemented to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subpart D
- **A3** - Credentials, other than UserID, for accounts with privileges sufficient to access or modify IT system data are encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B, when credentials are stored or transmitted
- **A4** - Credentials, other than UserID, for accounts with privileges sufficient to access or modify IT system configuration are encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B, when credentials are stored or transmitted

NFR – Security - awareness and training

- **B1** - IT system administrator(s) must complete applicable modules from information security training program

Subpart D. Data confidentiality high (C-High)

Include all of *data confidentiality minimum, low, and medium,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum, low or medium, or it may be a new requirement:

NFR – Security - configuration integrity

- **A1** - A non-refutable log of all access and modifications to IT system configuration will exist that contains action performed, individual, IP address, date, and time for a period of one year
- **A2** - Administrative activities that could result in the ability for a single person to commit or conceal fraud must be distributed to more than one individual
- **A3** - The incident response process, as defined in Operating Instructions 5.23.1.4, is tested annually

NFR – Security - configuration assessment

- **A1** - An independent third party will actively verify the configuration of the IT system at intervals no longer than three (3) years
- **A2** - An independent third party will actively verify the security of the application at intervals no longer than three (3) years
- **A3** - The security of application code will be verified by automated rule-based systems at intervals no longer than 365 days
- **A4** - The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than seven (7) days

NFR – Security - data access

- **A1** - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration or highly restricted or restricted IT system-managed data
- **A2** - Individual access to the IT system and data is reviewed every six (6) months
- **A3** - Default deny logical controls exist between all security perimeters

NFR – Security - data classification

- **A1** - Individual elements of the data managed by the IT system have assigned owners
- **A2** - Each data element of the IT system has been classified as either highly restricted, restricted, or low

NFR – Security - data encryption

- **A1** - Data classified as Highly restricted or restricted is encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B, when stored, transported, or transmitted

NFR – Security – awareness and training

- **A1** – IT system administrator(s) must have, or be under the guidance of an individual who has, an applicable industry-accepted certification or no less than five (5) years of experience implementing, managing, or maintaining a similar IT system

Subpart E. Data integrity minimum (I-Minimum)

NFR – Security - configuration integrity

- **D2** - The IT system will meet Operating Instructions 5.23.1.8 Anti-malware Installation and Management
- **D4** - IT systems preforming storage, business logic, or unencrypted transmission of data classified as highly restricted or restricted must be administered by personnel using least privilege

NFR – Security - configuration assessment

- **D1** - The configuration of the IT system will meet a documented standard or benchmark
- **D2** - The IT system patch intervals will meet requirements in Operating Instructions 5.23.1.5 Security Patch Management

NFR - Security - data access

- **D1** - A process for granting and revoking logical and physical access is implemented
- **D2** - Credentials used to access the IT system or data meet controls and guidance defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3

- **D3** - Logical and physical security perimeters are identified and documented
- **D4** - The IT systems storing or managing the data will have network segmentation controls implemented to meet controls and guidance defined in ISO 27002, section 13.1.3

NFR – Recoverability - configuration

- **D1** - No more than one business day of data modifications will be lost

NFR – Recoverability - logical

- **D1** - The recovered IT system will meet all pre-failure functional and non-functional requirements

Subpart F. Data integrity low (I-Low)

Include all of *data integrity minimum,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum, or it may be a new requirement:

NFR – Security - configuration assessment

- **C1** - The configuration of the IT system will be verified by automated rule based systems at intervals no longer than 90 days
- **C2** - An automated, systematic means of mitigating software vulnerabilities must exist.
- **C3** - The configuration of the IT system will meet a current vendor-provided standard or benchmark
- **C4** - Modification of IT system configuration is restricted to individuals that meet security - awareness and training non-functional requirement

NFR – Security - data access

- **C1** - IT system administrator and user access is logged
- **C2** - Individual access to the IT system and data is reviewed annually
- **C3** - Unique credentials are required for each individual accessing the data
- **C5** - Logical controls exist that enforce a default deny policy from lower to higher security perimeters

NFR – Recoverability - logical

- **C1** - The IT system must have defined and published recovery point and recovery time objectives

Subpart G. Data integrity medium (I-Medium)

Include all of *data integrity minimum and low,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum or low, or it may be a new requirement:

NFR – Security - configuration integrity

- **B1** - A non-refutable log of all access and modifications to IT system configuration by accounts with privileges sufficient to modify IT system configuration will exist and contain action performed, individual, IP address, date, and time for a period of one year

- **B2** - No more than one business day of IT system modifications will be lost
- **B3** - Access and modification of IT system configuration will be conducted using privileges limited to the minimum required to complete the activity

NFR – Security - configuration assessment

- **B1** - The configuration of the IT system will be verified by automated rule based systems at intervals no longer than 30 days
- **B2** - The configuration of the IT system will be compared against Center for Internet Security (CIS) level 1 or equivalent and differences documented
- **B3** - A formal process exists for assessing configuration modifications prior to implementation

NFR – Security - Data access

- **B1** - The IT system will maintain a non-refutable log of all access and modifications to highly restricted IT system-managed data sufficient to determine the individual, IP address, date, and time
- **B3** - Tools and processes exist that detect, log, and alert on unauthorized access to the IT system and to data managed by the IT system
- **B5** - Access to data is based on assigned roles
- **B7** - System accounts will conform to meet controls and guidance defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3

NFR – Recoverability - configuration

- **B2** - No more than the most recent fifteen minutes of data modifications will be lost

NFR – Recoverability - logical

- **B2** - No more than the most recent one business day of data modifications will be lost

Subpart H. Data integrity high (I-High)

Include all of *data integrity minimum, low and medium,* plus the following. In some cases, the requirement may be an addition to a requirement previously defined under minimum, low or medium, or it may be a new requirement:

NFR – Security - configuration integrity

- **A1** - A non-refutable log of all access and modifications to IT system configuration will exist that contains action performed, individual, IP address, date, and time for a period of one year
- **A2** - Administrative activities that could result in the ability for a single person to commit or conceal fraud must be distributed to more than one individual.

NFR – Security - configuration assessment

- **A1** - An independent third party will actively verify the configuration of the IT system at intervals no longer than three (3) years
- **A2** - An independent third party will actively verify the security of the application at intervals no longer than three (3) years
- **A3** – The security of application code will be verified by automated rule-based systems at intervals no longer than 365 days
- **A4** – The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than seven (7) days

NFR – Security - Data Access

- **A3** - Default deny logical controls exist between all security perimeters
- **B2** - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration

NFR – Recoverability - Configuration

- **A2** - No data modifications will be lost

NFR – Recoverability - Logical

- **A1** - No more than the most recent one hour of data modifications will be lost

Appendix A
NFR - Recoverability – Configuration

Category: Recoverability

Context: Configuration

Goals: When an IT system becomes unavailable as a result of a modification of the configuration of the IT system, the system must be recoverable to a pre-failure state using a pre-determined configuration, within a pre-established elapsed time, and with an acceptable level of data loss. The recovered IT system configuration must be identical to the pre-failed state.

Rationale: If the availability of the IT system is sufficiently critical, the IT system must be capable of being recovered from failed configuration changes within a reasonable time frame and with functionality identical to its pre-failure state.

Requirement: Failure of an IT system because of modification of the configuration of the system must not cause user-detectable loss of business functionality for an elapsed time more than *metric*. After an elapsed time no longer than *metric* (see below), the user will be able to resume pre-failed state business functionality with data loss no more than *metric*.

Metric:
Level A:

A1 - The user detectable loss of functionality will be for an elapsed time of no more than four business hours
A2 - No data modifications will be lost
A3 - A formal process exists for determining the root cause of a failed configuration modification

Level B:

B1 - The user-detectable loss of business functionality will be an elapsed time of no more than one business day
B2 - No more than the most recent fifteen minutes of data modifications will be lost
B3 - A formal process exists for review and testing of configuration modifications

Level C:

This level intentionally left blank

Level D:

D1 - No more than one (1) business day of data modifications will be lost
D2 - The recovered IT system will meet pre-failure functional and non-functional requirements

Scale: Elapsed time, availability: hours duration. elapsed time, data loss: minutes duration

Stakeholders: IT system managers, operations, IT system users

Implications: If this requirement is not met, the organization will incur significant risk of loss of business functionality and data in the event of failed configuration modifications. Additionally, if this requirement is not met, the IT system is subject to extended application outages during system maintenance and upgrades.

Appendix B

NFR - Recoverability – Logical

Category: Recoverability

Context: Logical

Goals: When an IT system becomes unavailable because of a modification of business data outside of normal business processes, the system must be recoverable to a pre-failure state within a pre-established elapsed time, and with an acceptable data loss. The recovered IT system must be capable of meeting all pre-failure functional and non-functional requirements.

Rationale: If the availability or integrity of the IT system is sufficiently critical, the system must be capable of being recovered from modification of business data within a reasonable time frame and with functionality identical to a pre-failure state.

Requirement: Modification of business data outside of normal business process must not cause user detectable loss of business functionality for an elapsed time more than *metric* (see below). After an elapsed time no longer than *metric*, the user will be able to resume business functionality with data loss no more than *metric*.

Metric:

Level A:

A1 - No more than the most recent one (1) hour of data modifications will be lost

Level B:

B1 - The user-detectable loss of business functionality will be an elapsed time of no more than one business day

B2 - No more than the most recent one (1) business day of data modifications will be lost

Level C:

C1 - The IT system must have defined and published recovery point and recovery time objectives

Level D:

D1 - The recovered IT system will meet all pre-failure functional and non-functional requirements

Scale: Elapsed time, availability: duration, elapsed time, data loss: duration

Stakeholders: IT system managers, operations, IT system users

Implications: If this requirement is not met, the organization will incur significant risk of extended loss of business functionality in the event of unplanned or failed data modifications.

Appendix C
NFR – Security – Awareness and Training

Category: Security

Context: Awareness and training

Goals: IT system administrative personnel have the knowledge and skills to effectively implement, manage, and maintain the IT system sufficient to meet non-functional requirements.

Rationale: IT system administrative personnel must have the skills, knowledge and/or experience to effectively implement requirements defined by federal or state law, statute, regulations, contractual agreements, board policies, system procedures or operating instructions, and non-functional requirements.

Requirement: IT system administrative personnel must have knowledge, skills, and/or experience according to *metric* (see below).

Metric:

Level A:

A1 - IT system administrator(s) must have, or be under the guidance of an individual who has, an applicable industry accepted certification or no less than five (5) years of experience implementing, managing, or maintaining a similar IT system

Level B:

B1 - IT system administrator(s) must complete applicable modules from *information security training program*

Level C:

C1 - IT system administrator(s) must be offered at least 40 hours of job related formal training per year

C2 - IT system administrator(s) must complete Public Jobs: Private Data courses: *Data Security in Your Job*, *Securing Your Computer Workstation* and *Using Data in the Workplace, Data Security for Faculty, Managers and Supervisors, Managing Student Data Securely, Managing Financial Data Securely* and *Managing Personnel Data Securely* annually

Level D:

D1 - IT system administrator(s) must complete Public Jobs: Private Data courses: *Data Security in Your Job*, *Securing Your Computer Workstation* and *Using Data in the Workplace*

Scale: Training hours, industry certifications, years of experience

Stakeholders: IT system managers, operations
Implications: If this requirement is not met, the organization will incur increased risk of person-induced security and availability incidents.

Appendix D

NFR – Security – Configuration Assessment

Category: Security

Context: Configuration assessment

Goals: An IT systems initial configuration must be resistant to unauthorized access or modification of configuration and data. The IT system must be maintained in a resistant configuration for the life of the system, and must be verified by appropriate means. IT system administration activities must be conducted with privileges limited to the minimum required to complete the activity.

Rationale: If the confidentiality and integrity of the data managed by the IT system is critical, the system must be configured and maintained in a secure state, resistant to unauthorized configuration and data modifications. To ensure that the IT system is maintained in that state, the configuration of the system must be verified at periodic intervals.

Requirement: The IT system must be configured to *metric* (see below). The configuration must be verified to *metric*. Administrative functions must be conducted according to *metric*.

Metric:

Level A:

A1 - An independent third party will actively verify the configuration of the IT system at intervals no longer than three (3) years
A2 - An independent third party will actively verify the security of the application at intervals no longer than three (3) years
A3 – The security of application code will be verified by automated rule-based systems at intervals no longer than 365 days
A4 – The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than seven (7) days

Level B:

B1 - The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than 30 days.
B2 - The configuration of the IT system will be compared against Center for Internet Security (CIS) level 1 or equivalent and differences documented
B3 - A formal process exists for assessing configuration modifications prior to implementation

Level C:

C1 - The configuration of the IT system will be verified by automated rule-based systems at intervals no longer than 90 days

C2 - An automated, systematic means of mitigating software vulnerabilities must exist
C3 - The configuration of the IT system will meet a current vendor provided standard or benchmark
C4 - Modification of IT system configuration is restricted to individuals that meet security – awareness and training non-functional requirement

Level D:

D1 - The configuration of the IT system will meet a documented standard or benchmark
D2 - The IT system patch intervals will meet requirements in Operating Instructions 5.23.1.5 Security Patch Management

Scale:

Configuration standard: Center for Internet Security (CIS) Benchmark
Patch Management Interval: Duration, Operating Instructions 5.23.1.5 Security Patch Management
Configuration assessment: interval, days

Stakeholders: IT system managers, operations, IT system users

Implications: If this requirement is not met, the organization will incur significant risk of extended loss of business functionality in the event of unplanned configuration-related outages.

Appendix E
NFR – Security – Configuration Integrity

Category: Security

Context: Configuration integrity

Goals: When the configuration of an IT system is modified outside of normal processes, the system must be able to detect the unauthorized modification, and must be recoverable to a pre-modified state using a pre-determined configuration. No more than an acceptable data loss should result from the unplanned configuration. The recovered IT system must be capable of meeting all pre-modification functional and non-functional requirements. Sufficient logging and auditing must be in place to determine the source of the modification. The response to unauthorized modification must follow a pre-determined process or plan.

Rationale: If the confidentiality and integrity of the data managed by the IT system is sufficiently critical, the system must have the ability to prevent unauthorized modifications to IT system configuration and data, the IT system must be able to determine the source of system modifications, and the system must be capable of being recovered from unauthorized configuration changes with functionality identical to a pre-modified state.

Requirement: Unauthorized modification of the configuration of the IT system and system-managed data must be recoverable to a point in time of *metric* (see below). IT system changes will be logged to *metric*. The response to modification of IT system configuration or system managed data must meet *metric*.

Metric:

Level A:

A1 - A non-refutable log of all access and modifications to IT system configuration will exist that contains action performed, individual, IP address, date, and time for a period of one (1) year

A2 - Administrative activities that could result in the ability for a single person to commit or conceal fraud must be distributed to more than one individual

A3 - The incident response process, as defined in Operating Instructions 5.23.1.4 Information Security Incident Response, is tested annually

Level B:

B1 - A non-refutable log of all access and modifications to IT system configuration by accounts with privileges sufficient to modify IT system configuration will exist and contain action performed, individual, IP address, date and time for a period of one year

B2 - No more than one (1) business day of IT system modifications will be lost

B3 - Access and modification of IT system configuration will be conducted using privileges limited to the minimum required to complete the activity

Level C:

This level intentionally left blank

Level D:

D1 - The recovered IT system will meet all pre-modification functional and non-functional requirements

D2 - The IT system will meet Operating Instructions 5.23.1.8 Anti-malware Installation and Management

D3 - A process exists that meets Operating Instructions 5.23.1.4 Information Security Incident Response

D4 - IT systems performing storage, business logic, or unencrypted transmission of data classified as highly restricted or restricted must be administered by personnel using least privilege

Scale:

Log content: log contains action performed, individual, IP address, date, and time
Log retention: duration, days

Stakeholders: IT system managers, operations, IT system users

Implications: If this requirement is not met, the organization will incur significant risk of loss of business functionality and data in the event of unplanned configuration modifications.

Appendix F
NFR – Security – Data Access

Category: Security

Context: Data access

Goals: An IT system must have the ability to control and monitor access and modification to a system and the data managed by the IT system. The ability to access and modify the data must be limited to authorized individuals. The authorization must be dependent on current work assignment, job function, or other business requirement.

Rationale: Limiting an individual's access to only the IT systems and data they need to complete work assignments or job duties mitigates inappropriate access or modification of highly restricted or restricted data.

Requirement: Access to data must be granted to individuals by the data owner or person authorized to grant access. Access must be revoked when it is no longer required for the individual's work assignment or job duties. Logging of access must be implemented to *metric* (see below). Security controls must be implemented to *metric*.

Metric:
Level A:

A1 - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration or highly restricted or restricted IT system-managed data
A2 - Individual access to the IT system and data is reviewed every six (6) months
A3 - Default deny logical controls exist between all security perimeters

Level B:

B1 - The IT system will maintain a non-refutable log of all access and modifications to highly restricted IT system managed data sufficient to determine the individual, IP address, date, and time
B2 - Multi-factor authentication is required for each individual accessing or modifying the IT system configuration
B3 - Tools and processes exist that detect, log, and alert on unauthorized access to the IT system and to data managed by the system
B4 - When work assignments change, access is updated to reflect new work assignment
B5 - Access to data is based on assigned roles
B6 - Documented business or functional requirements identify the privileges required to perform all business functions that access or modify highly restricted or restricted data
B7 - System accounts will conform to meet controls and guidance defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3

Level C:

C1 - IT system administrator and user access is logged
C2 - Individual access to the IT system and data is reviewed annually
C3 - Unique credentials are required for each individual accessing the data
C4 - A documented relationship exists between data owner and data custodian
C5 - Logical controls exist that enforce a default deny policy from lower to higher security perimeters

Level D:

D1 - A process for granting and revoking logical and physical access is implemented
D2 - Credentials used to access the IT system or data meet controls and guidance defined in International Standards Organization (ISO) 27002, sections 9.4.2 and 9.4.3
D3 - Logical and physical security perimeters are identified and documented
D4 - The IT systems storing or managing the data will have network segmentation controls implemented to meet controls and guidance defined in ISO 27002, section 13.1.3

Scale: N/A

Stakeholders: Data owners, IT system managers, operations

Implications: If this requirement is not met, the appropriate security controls may not be implemented to protect the data from unauthorized access or improper data exposure.

Appendix G
NFR – Security – Data Classification

Category: Security

Context: Data classification

Goals: All data must have an assigned owner or business department and be classified both to protect the confidentiality and integrity of the data and to comply with applicable state and federal laws and regulations.

Rationale: Implementing security controls requires data ownership and classification so the appropriate controls can be implemented commensurate with the classification level. Data owners have primary authority and accountability for the data.

Requirement: In addition to state and federal laws, regulations, statutes, and contractual agreements, applicable data must have an owner and be classified to *metric* (see below).

Metric:
Level A:

A1 - Individual elements of the data managed by the IT system have assigned owners
A2 - Each data element of the IT system has been classified as either highly restricted, restricted, or low

Level B:

This level intentionally left blank

Level C:

This level intentionally left blank

Level D:

D1 - The data managed by the IT system has an assigned owner
D2 - The data managed by the IT system has been classified as highly restricted, restricted, or low

Scale:

- **Low** - Data that by law are available to the public upon request
- **Restricted** - Data that by law is not public data and are available within the system/institution only to those with a legitimate need to know or, the data is so highly sensitive that the loss of confidentiality of the data will require statutory notification to affected parties (i.e., breach notification)
- **Highly Restricted** - Data that includes elements (1) for which loss of confidentiality is sufficient to assume a person’s identity in financial transactions; or (2) by law,

regulation, or contract requires high-level security controls; or (3) the loss of confidentiality could cause significant personal or institutional harm

Stakeholders: Data owners, data custodians, IT system managers, operations

Implications: If this requirement is not met, the appropriate security controls may not be implemented to protect the data accordingly, which could result in a loss of data integrity or unauthorized exposure.

Appendix H
NFR – Security – Data Encryption

Category: Security

Context: Data encryption

Goals: Data classified as highly restricted or restricted must not be exposed to unauthorized parties. When highly restricted or restricted data is stored or transmitted in a manner that may result in exposure, the data must be rendered unreadable to the unauthorized party.

Rationale: Data custodians are obligated to minimize the probability of unintentional exposure of highly restricted or restricted data to unauthorized parties.

Requirement: When data classified as highly restricted or restricted is stored outside of a higher risk network or perimeter, the data will be stored unreadable to *metric* (see below). When data classified as highly restricted or restricted is physically or logically transported or transmitted outside of a higher risk network or perimeter, the data will be rendered non-readable to *metric.*

Metric:

Level A:

A1 - Data classified as highly restricted or restricted is encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B when stored, transported or transmitted

A2 - Key recovery for symmetric keys will be implemented to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subpart D

A3 - Credentials, other than UserID, for accounts with privileges sufficient to access or modify IT system data are encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B, when credentials are stored or transmitted

A4 - Credentials, other than UserID, for accounts with privileges sufficient to access or modify IT system configuration are encrypted to meet requirements in Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subparts A and B, when credentials are stored or transmitted

Level B:

B1 - Credentials, other than UserID, for accounts with privileges sufficient to modify IT system configuration are encrypted when stored or transmitted.

Level C:

This level intentionally left blank

Level D:

D1 - IT system is implemented in conformance with network segmentation policies/controls implemented to meet requirements defined in ISO 27002, section 13.1.3
D2 - Logical and physical security perimeters are identified and documented
D3 - Data classified as highly restricted or restricted stored, transported, or transmitted to a higher risk network or perimeter is encrypted

Scale:

Transport Encryption:
Storage Encryption: Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subpart A and B
Key Recovery: Operating Instructions 5.23.1.2 Encryption for Mobile Computing and Storage, Devices, Subpart D

Stakeholders: Data owners, IT system managers, operations

Implications: If this requirement is not met, the appropriate security controls may not be implemented to protect the data from unauthorized access or improper data exposure.

Part 6. Implementation schedule

Implementation Requirement	**Required Date of Implementation**
High Assurance Profile IT systems or services	Within eighteen (18) months from date of operating instructions adoption
Medium, Low and Minimum Assurance Profile IT systems or services	Within twenty-four (24) months from date of operating instructions adoption

Related Documents:

- Please refer to the website for a list of Related Documents.

Operating Instruction History:

Date of Adoption: 03/08/17
Date of Implementation: 03/08/17 (see Part 6 Implementation schedule)
Date of Last Review:

Date and Subject of Amendments:
No additional HISTORY.