New York State Information Technology Standard	No: NYS-S14-002
IT Standard: **Information Classification**	**Updated:** 07/16/2020
	Issued By: NYS Office of Information Technology Services
	Owner: Chief Information Security Office

1.0 Purpose and Benefits

This standard outlines a classification process and provides procedures for classifying information in a manner that uniformly protects information entrusted to New York State (NYS) State Entities (SE).

The process of classifying information pursuant to this standard may serve as a basis for a SE to evaluate the retention and disposition schedules currently in effect for its records and, where appropriate, consider revising those schedules to manage the records that must be protected by the SE. Similarly, the classification process can facilitate the accurate and efficient application of the exemptions from disclosure enumerated in NYS Public Officers Law, Article 6 Freedom of Information Law by providing a framework for a comprehensive assessment of the SE's information assets.

2.0 Authority

Section 103(10) of the State Technology Law provides the Office of Information Technology Services ("ITS") with the authority to establish statewide technology policies, including technology and security standards. *Section 2 of Executive Order No. 117* provides the State Chief Information Officer with the authority to oversee, direct and coordinate the establishment of information technology policies, protocols and standards for State government, including hardware, software, security and business re-engineering. Details regarding this authority can be found in NYS ITS Policy, *NYS-P08-002 Authority to Establish State Enterprise Information Technology (IT) Policy, Standards and Guidelines*.

3.0 Scope

This standard applies to all SEs, defined as "State Government" entities as defined in Executive Order 117, established January 2002, or "State Agencies" as defined in Section 101 of the State Technology Law. This includes employees and all third parties (such as local governments, consultants, vendors, and contractors) that use or access any IT resource for which the SE has administrative responsibility, including systems managed or hosted by third parties on behalf of the SE. While an SE may adopt a different standard, it must include the requirements set forth in this one.

The scope of this standard includes information through its entire life cycle (i.e., generation, use, storage, and disposition). It covers information in any form including electronic, paper, voice, video, or other physical forms.

4.0 Information Statement

As per the NYS-P03-002 Information Security Policy, all information and/or information systems must be classified.

Information classification is based on three principles of security: 1) confidentiality, 2) integrity, and 3) availability. For each principle, information can be classified as low, moderate, or high based on the potential impact on the SE should certain events occur that jeopardizes the information and/or information systems needed by the SE. When classifying the impact, the SE should consider how the information/ information systems is used to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Impact levels are defined as limited, serious, and severe or catastrophic. For the purposes of classification, limited impact shall be deemed to include no impact.

Potential Impact	Definitions
Low	The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. A limited adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Moderate	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. A serious adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
High	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Figure 1: Potential Impact Levels - National Institute of Standards and Technology (NIST) Special Publication 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

Each SE should review the impact levels in the context of its own operational environment. Figure 2 shows the *Information Asset Classification Categories*.

	INFORMATION CLASSIFICATION CATEGORIES per FIPS 199		
	LOW	**MODERATE**	**HIGH**
CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust	The unauthorized disclosure of information could be expected to have **limited or no impact** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious impact** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.
INTEGRITY Consider impact of unauthorized modification or destruction on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust	The unauthorized modification or destruction of information could be expected to have **limited** or **no impact** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious impact** on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.
AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs ▪ Public Trust	The disruption of access to or use of information or an Information System could be expected to have **limited** or **no impact** 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 impact** 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 **severe** or **catastrophic impact** on organizational operations, organizational assets, or individuals.

Figure 2: Information Asset Classification Matrix - National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems

Information Classification Process

The information classification process must include the following:

1. Identification of information assets;

2. Classification of information assets; by confidentiality, integrity, and availability ("CIA"); and

3. Determining controls based upon the classification.

1. Identification of Information Assets

Identification of information assets involves creating an inventory of all information assets in the SE. The following items need to be considered when constructing this inventory:

A. Grouping of information assets

B. Determining the information owner

C. Determining the information custodian

D. Identifying information assets

A. Grouping of Information Assets

To facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to appropriately group information assets together. A broad grouping may result in applying controls unnecessarily as the asset must be classified at the highest level necessitated by its individual data elements. For example, if a Human Resources unit decides to classify all of their personnel files as a single information asset and any one of those files contains a name and social security number, the entire grouping would need to be protected with moderate confidentiality controls.

A narrow grouping allows for more precise targeting of controls. However, as there are more information assets to classify, this increases the complexity of the classification and the management of controls. Using the previous example, classifying the multitude of personnel files (e.g., appointment letters, timecards, position classifications, holiday waivers) as individual information assets requires a different set of controls for each classification.

In the case of an information technology system, such as a database, data warehouse, or application server, while it may be easier to apply a single set of controls as a result of classifying the system as a single entity, costs may be reduced by applying the controls to the individual elements, such as specific fields, records, or applications. Therefore, it is important that the SE evaluate the risk and cost benefit of grouping a given set of assets.

B. Determining the Information Owner

Responsibility for the classification and definition of controls for an information asset belongs to an individual in a managerial position who is ultimately responsible for the confidentiality, integrity, and availability of that information. If multiple individuals are found to be "owners" of the same information asset, a single individual owner must be designated by a higher level of management. The information owner is responsible for determining the information's classification, how and by whom the information will be used. Owners must understand the uses and risks associated with the information for which they are responsible and any laws, regulations, or policies which govern access and use. Each owner must exercise due diligence with respect to the proper classification of data in order to prevent improper disclosure and access.

C. Determining the Information Custodian

Information custodians are people, units, or organizations responsible for implementing the authorized controls for information assets based on the classification level. An information asset may have multiple custodians. Based on the information owner's requirements, the custodian secures the information, applying safeguards appropriate to the information's classification level. Information custodians can be from within the SE or from third parties (e.g., another SE or non-SE). If the custodian is a third party, a formal, written agreement between the custodian's organization and the SE that owns the information must specify the responsibilities of each party. An information custodian may also be the information owner.

D. Identifying Information Assets

For each information asset in their control, the information owner must identify at a minimum:

- Source of the information asset (e.g., unit, agency)
- Use of the information asset (i.e., purpose/business function)
- Business processes dependent on the information asset
- Users/groups of users of the information asset

2. Classification of Information Assets

Owners must answer the questions in the Information Asset Classification Worksheet (Appendix A) to determine the classification of their information assets. It is appropriate to recruit and work with subject matter experts who have specific knowledge about the information asset, such as Counsel's Office and the Records Management Officer. The Information Security Officer (ISO)/designated security representative may also be called upon to advise and assist the information owner in determining the classification. A SE may add more questions to the Information Asset Classification Worksheet but may not alter or remove the original questions.

Information assets are classified according to confidentiality, integrity, and availability. Each of these three principles of security is individually rated as low, moderate, or high.

For example, an information asset may have a confidentiality level of "high", an integrity level of "moderate", and an availability level of "low" (e.g., HML).

Questions are categorized by confidentiality, integrity, and availability. Each question must be answered sequentially, to the best of the information owners' abilities.

5.0 Compliance

This standard shall take effect upon publication. Compliance is expected with all enterprise policies and standards. ITS may amend its policies and standards at any time; compliance with amended policies and standards is expected.

If compliance with this standard is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, SEs shall request an exception through the Chief Information Security Office exception process.

6.0 Definitions of Key Terms

Except for terms defined in this policy, all terms shall have the meanings found in http://www.its.ny.gov/glossary.

Term	Definition
Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

7.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:

Chief Information Security Office
Reference: NYS-S14-002
NYS Office of Information Technology Services
1220 Washington Avenue, Building 5
Albany, NY 12226
Telephone: (518) 242-5200
Email: CISO@its.ny.gov

Statewide technology policies, standards, and guidelines may be found at the following website: http://www.its.ny.gov/tables/technologypolicyindex

8.0 Revision History

This standard shall be reviewed at least once every year to ensure relevancy.

Date	Description of Change	Reviewer
10/10/2008	Original Standard Release (*released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)*)	
1/17/2014	Rebranded for the Office of Information Technology Services; (*replaces CSCIC/OCS PS08-001 Information Classification and Control*); split into two standards – Information Classification and Information Security Controls	Thomas Smith, Chief Information Security Officer
6/20/2014	Addition of Appendix B: Information Classification Supplemental Guidance and Appendix C: Information Asset Identification Worksheet	Deborah A. Snyder, Acting Chief Information Security Officer
9/19/2014	Updated wording in Determination of Controls section to point to NIST 800-53 as well as the NYS Information Security Controls Standard and clarify that control selection is based on risk; added hyperlink to footnote under Figure 1; added NYS Risk Management Standard as a reference	Deborah A. Snyder, Acting Chief Information Security Officer
03/10/2017	Updated Scope, contact information and rebranding	Deborah A. Snyder, Deputy Chief Information Security Officer
07/16/2020	Update revised Scope and Authority and update links from Identity Assurance to Digital Identity	Karen Sorady, Chief Information Security Officer

05/19/2021	Update Scope language	Karen Sorady, Chief Information Security Officer

9.0 Related Documents

[Federal Information Processing Standards (FIPS) Publication 199: Standards for Security Categorization of Federal Information and Information Systems](#)

[NYS-S14-001 Information Security Risk Management Standard](#)

[NIST Special Publication 800-60 Volume 1, Revision 1](#)

[NYS-P10-006 Digital Identity Policy](#)

[NYS-S13-004 Digital Identity Standard](#)

Appendix A

Section One: Information Asset Identification Worksheet

Instructions:

Record the requested information for the information asset you are classifying. Job titles, in place of named individuals, can be used where appropriate for ease of maintenance.

Completed By:

_____

Completed Date:

_____

Name of Information Asset:

_____

Information Asset Description/Comment:

_____

Information Asset Use:

_____

Information Asset Format:
(i.e., paper, electronic)

_____

Information Asset Storage:
(e.g., file cabinet, safe, database, network share, CD/DVD, portable drive)

_____

Source of Information:

_____

Business Process(es) Supported:

_____

Information Owner:

_____

Information Custodian:

_____

Internal Information User(s):

_____

External Information User(s):
(e.g., other State Agencies, other government agencies, public)

_____

Information Asset ID Number:

_____

SECTION TWO: INFORMATION ASSET CLASSIFICATION WORKSHEET

Instructions for rating each section
If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

CONFIDENTIALITY QUESTIONS				
1. Is the information publicly available?	**No**		**Yes**	
2. Does the information include or contain PPSI **(Personal, Private, or Sensitive Information)?**	**No**		**Yes**	
	None	**Limited**	**Serious**	**Severe**
3. What impact does unauthorized disclosure of information have on health and personal safety?				
4. What is the financial or agency liability impact of unauthorized disclosure of information?				
5. What impact does unauthorized release of sensitive information have on the SE mission?				
6. What impact does unauthorized disclosure of information have on the public trust, agency reputation, and public interests?				
7. Is confidentiality mandated by law or regulation? If yes, what is the impact of unauthorized disclosure of information. If no, do not make a selection.				
8. Is the information intended for limited distribution? If yes, what is the impact of unauthorized disclosure. If no, do not make a selection				
CONFIDENTIALITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

INTEGRITY QUESTIONS				
1. Does the information include medical records	No		Yes	
2. Is the information (e.g., security logs) relied upon to make critical security decisions?	No		Yes	

	None	Limited	Serious	Severe
3. What impact does unauthorized modification or destruction of information have on health and safety?				
4. What is the financial impact of unauthorized modification or destruction of information?				
5. What impact does unauthorized modification or destruction of information have on the SE mission?				
6. What impact does unauthorized modification or destruction have on the public trust?				
7. Is integrity addressed by law or regulation? If yes, what is the impact of unauthorized modification or destruction of information. If no, do not make a selection.				
8. Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, what is the impact of unauthorized modification or destruction of information. If no, do not make a selection.				
INTEGRITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

AVAILABILITY QUESTIONS			
Assessment Question			
	As time permits	**Within 1 to 7 days**	**24 hrs. per day/7 days a week**
1. This information needs to be available:			
Impact Questions			
	None	**Limited**	**Serious**	**Severe**
2. What is the impact to health and safety if the information were not available when needed?				
3. What is the financial impact if the information were not available when needed?				
4. What is the impact to the SE mission if the information were not available when needed?				
5. What is the impact to public trust if the information were not available when needed?				
AVAILABILITY RATING				

If ALL answers are **GREEN**, the rating is **Low**; if ANY of the answers are **YELLOW** and **NONE** are **RED**, the rating is **MODERATE**; if ANY of the answers are **RED**, the rating is **HIGH**.

_____   _____

Information Owner - print   **Date**

_____

Information Owner - signature

_____   _____

ISO/Designated security representative - print   **Date**

_____

ISO/Designated security representative - signature

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

Introduction

The classification of information will be the basis for many information security decisions in an organization. Before deciding the level of resources (e.g., money, time, and technology) required for protection, it is essential that you know what information needs to be protected and the level of protection that is required. The purpose of this supplement is to provide additional guidance on the information classification process.

Identifying Information Assets
An efficient approach towards identifying information assets is for information owners to maintain an inventory for each information asset in their control. The inventory should minimally include the following:

1. Source of the information asset (e.g., unit, agency)
2. Use of the information asset (e.g., purpose/business function)
3. Business processes dependent on the information asset
4. Users/groups of users of the information asset
5. Owner of the information asset

Information assets can be identified using the template provided in Section One of Appendix A or this information can be extracted from an existing information inventory, if available. Job titles, in place of named individuals, can be used for the custodian, owner, and users in order to ease maintenance of your information asset inventory. Samples of completed templates are provided below in Figures 1 and 2.

Information Asset Identification	
Completed By:	Peter Pasquale, Assistant Director, Finance Unit
Completed Date:	10/10/2008
Department:	Finance
Name of Information Asset:	Purchase Requisition
Information Asset Description/Comment:	Purchase Requisition
Information Asset Use:	Track purchases
Information Asset Format:	Electronic
Information Asset Storage:	Financial Management System Database
Source of Information:	Requisition and Order Processing Unit
Business Process(es) Supported:	Budget/Finance
Information Owner:	Peter Pasquale
Information Custodian:	Financial Management System Database Administrator
Internal Information User(s):	Finance Unit
External Information User(s):	None
Information Asset ID Number:	500

Figure 1: Information Asset Identification Template by Single Asset

Information Asset Identification	
Completed By:	Peter Pasquale, Assistant Director, Finance Unit
Completed Date:	10/10/2008
Department:	Finance
Name of Information Asset:	Purchase Records Group
Information Asset Description/Comment:	Consists of Purchase Request, Purchase Quote, Purchase Requisition, Invoice, Payment Approval
Information Asset Use:	Track purchases
Information Asset Format:	Electronic, Paper
Information Asset Storage:	Financial Management System Database, Finance File Cabinet
Source of Information:	Requisition and Order Processing Unit
Business Process(es) Supported:	Budget/Finance
Information Owner:	Peter Pasquale
Information Custodian:	Financial Management System Database Administrator, Finance Unit
Internal Information User(s):	Finance Unit
External Information User(s):	None
Information Asset ID Number:	501

Figure 2: Information Asset Identification Template by Grouped Asset

Information Needed for Determining the Classification

Before determining the classification, it may be beneficial for the information owner to familiarize themselves with the following areas:

Source, Purpose, and Value:
- How the information asset is used in supporting business functions.
- How often the information asset is used.
- How often the information asset is updated.
- Dependencies between this information asset and others.
- The cost of creating and duplicating the information.

Legal Requirements:
- Laws, regulations, policies, or contracts that mandate special security requirements for the information (e.g., Health Insurance Portability and Accountability Act (HIPAA)).
- Retention requirements for the information asset.

Access Requirements:
- Who has/should have access to the information (e.g., people, positions, organizational units).
- Whether the information is shared among other units/State Entities, third-parties, Federal/local governments.

Health and Safety Concerns:
- Impact on State Entity employees as well as the public.

Mission:
- The overall mission of the State Entity.
- The information owner's role (or unit's role) in completing the mission.

Non-tangible Effects:
- Impact if information asset is not available (temporarily or permanently).
- The effect of a breach of confidentiality, integrity, or availability on the intangible assets of the State Entity such as reputation, trust and morale.

Classification of Information Assets

Classification of information assets is facilitated by the use of a series of questions. The answers will help determine the information asset classification.

The **Information Asset Classification Worksheet**, found in Appendix A, contains the confidentiality, integrity, and availability questions that must be answered when classifying information. Following are example answers to assist in determining the appropriate response.

Confidentiality Questions

[1] Is the information publicly available?

Example(s): Information that must be lawfully made available to the general public from Federal, State, or local government records or information that does not need to be withheld for security, legal or privacy concerns is generally deemed publicly available. Examples include public transportation schedules, a listing of local city events, or health improvement guidelines. These items would be ranked low in confidentiality.

[2] Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?

Example(s): A W-2 form contains a name, as well as a social security number. This would be considered private information and therefore have a minimum confidentiality of moderate, which may be adjusted based on responses to subsequent impact questions. See the NYS Information Technology Policies, Standards and Best Practice Guidelines Glossary for a definition of PPSI.

[3] What impact does unauthorized disclosure of information have on health and personal safety?

Example(s): There may be information which, if publicly released, may impact the health and personal safety of the State Entity's workforce and NYS citizens such as, the blueprint and drawings of critical infrastructure buildings, critical infrastructure related systems, network configurations, or disaster recovery/business continuity plans. These could be exploited by criminals to sabotage or destroy buildings, emergency services, or critical infrastructure operations resulting in a severe impact to health and personal safety of NYS citizens thereby placing these items in the high confidentiality category.

[4] What is the financial or agency liability impact of unauthorized disclosure of information?

Example(s): The State Entity may be exposed to litigation or regulatory fines due to disclosure of information protected by law or confidentiality agreements. For instance, unauthorized release of vendor bid information containing bidder's proprietary information could jeopardize the bidding process as well as potentially expose the State to litigation.

Similarly, if the investment decisions of the State's retirement system become known prior to their execution, it could alter the market sentiment ahead of the investment causing financial losses.

[5] What impact does unauthorized release of sensitive information have on the SE mission?

Example(s): An SE may be charged with ensuring that illegal goods do not enter State borders. As part of that mission, the SE may be responsible for collecting and maintaining information regarding unmanned border crossings. If there was an unauthorized release of that information, resulting in an increase of illegal traffic across State borders, it could have a severe impact on the SE's ability to fulfill its mission.

An example of limited impact would be the release of employee contact information which may result in additional phone calls/emails/office visits.

If a list of local delivery restaurants and their phone numbers is disclosed, there would be no impact.

[6] What impact does unauthorized disclosure of information have on the SE's intangible assets such as the public trust, agency reputation, and public interests?

Example(s): It is important for the government to maintain the public's trust. For example, the unauthorized exposure of medical records from a State-run facility could lead to a loss of the public trust in the State's ability to protect sensitive information.

An SE which collects and maintains the confidential records of citizens requires a high level of public trust. Unauthorized disclosure of data through the actions of a malicious insider, external hacker, or through a random accident could erode the public's trust in the SE and their ability to protect citizen data.

[7] Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized disclosure of information.

Example(s): Some types of information, including personal health records, student grades, and financial and personnel records may be protected by Federal, State, and local laws or regulations. Disclosing this information can lead to civil or criminal liability. There are several key statutes, such as HIPAA, that should be examined based on the information asset being classified.

[8] Is the information intended for limited distribution? If yes, determine the impact of the unauthorized disclosure of that information.

Example(s): Some information generated within a State Entity is for internal use only and is not meant to be disclosed externally. The confidentiality of such information varies considerably based on the information asset. Information, such as system security configurations, which, if released, could jeopardize the security of a State Entity's assets, would require high confidentiality controls.

Administrative information, such as procedures for travel approval, though not publicized outside the State Entity, would be information that the public could legitimately obtain and should be ranked as low in confidentiality.

Integrity Questions

[1] Does the information include medical records?

Example(s): In the case of a health care institution, it is important that medical records and medical history are accurate. For example, it may be important to know whether someone is allergic to specific medications so that they are not administered. In addition, it would be necessary to know whether a person has a particular illness or medical condition which would require special treatment. Malicious or accidental alteration of a patient's health records can cause serious health consequences for that individual. Medical records require a minimum integrity classification of moderate. This rating may be adjusted based on responses to subsequent questions.

[2] Is the information relied upon to make critical security decisions?

Example(s): It is important that security records (e.g., computer security logs, building security access logs) are accurate in order to verify legitimate access and identify unauthorized access attempts. Security related records require a minimum integrity classification of moderate. This rating may be adjusted based on responses to subsequent questions.

[3] What impact does unauthorized modification or destruction of information have on health and safety?

Example(s): There is a potential for severe impact on the safety of citizens if someone accesses an airline system and modifies the onboard navigation system.

The removal or editing of surveillance tapes may have a serious or severe impact depending on the presence of additional information provided by other forms of surveillance.
Something that could be of low to no impact on health and safety would be the unauthorized modification of an employee's calendars.

[4] What is the financial impact of unauthorized modification or destruction of information?

Example(s): There are many financial implications for the destruction or modification of information. It does not strictly mean monetary loss, but can also include loss of employee time and effort for recovery. Something that would have severe financial impact might be the loss of all financial records from a State Entity's financial management database.

If a database of vendor contact information was deleted, it would involve effort in re-creating the database. This would probably be of limited impact.

[5] What impact does unauthorized modification or destruction of information have on the SE mission?

Example(s): State Entity operations could be drastically affected if information is changed without authorization. For example, if someone removed all the phone numbers in a Do Not Call registry, it would severely impact the mission of the program to prevent unwanted calls to registered numbers.

The mission of a university is to provide education and certify the qualifications of students through academic degrees. Malicious or accidental changes to student academic records would have a severe impact on the university's mission of issuing academic credentials.

[6] What impact does unauthorized modification or destruction of information have on the public trust?

Example(s): The public relies on government to provide accurate information. Failure to do so would erode public trust. For example, if information on certification for licensed professionals was inaccurately modified without authorization and then posted to a public web site, the public would no longer trust the State Entity posting the information as a reputable source for this information.

[7] Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.

Example(s): Some types of information, including personal health records, student grades, and financial and personnel records, may be protected by Federal, State, and local laws. Allowing unauthorized changes to information may have legal consequences. There are several key statutes that should be examined based on the information asset being classified. For example, HIPAA requires safeguards to protect against threats to the integrity of electronic protected health information.

[8] Is the information (e.g., financial transactions, performance appraisals) relied upon to make business decisions? If yes, determine the impact of unauthorized modification or destruction of that information.

Example(s): It is important for financial information to remain reliable. Unauthorized changes to financial transactions (e.g., direct deposit, electronic funds transfer) could severely impact the financial stability of a State Entity.

Employee appraisal records are used to make important personnel decisions. Someone may attempt to falsify records in hopes of getting a promotion, alternate employment, or to diminish someone else's reputation and/or record. The impact to the State Entity could vary dependent upon the situation.

Availability Questions

[1] This information needs to be provided or available:
    As time permits
    Within 1 to 7 days
    24 hrs. per day/7 days a week

Example(s): Intrusion detection systems send event notifications so that an incident can be analyzed and escalated based on the level of threat. Since security is critical, and severe damage can be caused to State Entity data and networks, this operation is time critical and requires high availability (24 hrs. per day/7 days a week).

[2] What is the impact to health and safety if information were not available when needed?

Example(s): Medical records contain information (e.g., allergies, blood type, previous medications) which is critical for providing patients with accurate medical care. Lack of availability to this data during emergency medical care can lead to life threatening situations therefore placing these items in the high availability (24 hrs. per day/7 days a week) category.

[3] What is the financial impact if information were not available when needed?

Example(s): For any State Entity where online services generate revenue, a disruption of service can have a financial impact which could be deemed severe.

A personal computer system crash which can be solved by a simple reboot would have limited impact.

[4] What is the impact to the SE mission if information were not available when needed?

Example(s): Public transportation's mission is to get customers quickly and efficiently to various locations. If access to train, bus, and subway schedules was unavailable, this could lead to an inability of public transportation to fulfill its mission. The impact to its mission would be severe.

[5] What is the impact to the public trust if the information were not available when needed?

Example(s):   State Entities have spent considerable effort modernizing operations to include online services and encouraging the public to use these services. If these services were seriously degraded or disrupted, this could cause serious embarrassment to the State Entity resulting in a severe impact and an erosion of the public's trust in the SE and the online services. The availability in this case would be high.