



ANDREW M. CUOMO
Governor

State Capitol P.O. Box 2062
Albany, NY 12220-0062
www.its.ny.gov

BRIAN DIGMAN
NYS Chief Information Officer
Director, Office of IT Services

<p>New York State Information Technology Standard</p>	<p>No: NYS-S14-002</p>
<p>IT Standard:</p> <p>Information Classification</p>	<p>Updated: 09/19/2014</p>
	<p>Issued By: NYS ITS</p> <p>Standard Owner: Enterprise Information Security Office</p>

1.0 Purpose and Benefits of the Standard

This standard outlines a classification process and provides procedures for classifying information in order to uniformly protect information entrusted to New York State Entities (SEs).

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 as a means of managing 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 the Freedom of Information Law by providing a framework for a comprehensive assessment of the SE's information assets.

2.0 Enterprise IT Policy/Standard Statement

Section 2 of Executive Order No. 117 provides the State Chief Information Officer, who also serves as director of the Office of Information Technology Services (ITS), 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 (IT) Policy, Standards and Guidelines.

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

3.0 Scope

This standard is applicable to SEs, staff and all other affiliates (e.g., contractors, vendors, solution providers), which have access to or manage SE information. 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 New York State (NYS) [Information Security Policy](#), all information 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 which jeopardizes the information and/or information systems needed by the SE 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 purposes of classification, limited impact shall be deemed to include no impact.

Limited impact would:

- cause a degradation in mission capability to an extent and duration that the SE is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to SE or third party assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Serious impact would:

- cause a significant degradation in mission capability to an extent and duration that the SE is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to SE or third party assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.

Severe or catastrophic impact would:

- cause a degradation in or loss of mission capability to an extent and duration that the SE is not able to perform one or more of its primary functions;
- result in major damage to SE or third party assets;
- result in major financial loss; or
- result in catastrophic harm to individuals involving loss of life or serious life threatening injuries.

Each SE should review the impact levels in the context of its own operational environment. Figure 1 shows the *Information Asset Classification Matrix*.

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	MODERATE	HIGH
<p>CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	The unauthorized access or disclosure of information would have limited or no impact to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have serious impact to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI or other information would have a severe or catastrophic impact on the organization, its critical functions, workforce, business partners and/or its customers.
<p>INTEGRITY Consider impact of unauthorized modification or destruction on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust 	The unauthorized modification or destruction of information would have limited or no impact to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have serious impact to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a severe or catastrophic impact on the organization, its critical functions, workforce, business partners and/or its customers.
<p>AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as:</p> <ul style="list-style-type: none"> • Health and Safety • Financial Loss • SE Mission/Programs ▪ Public Trust 	The disruption of access to or use of information would have limited or no impact to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have serious impact to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a severe or catastrophic impact on the organization, its critical functions, workforce, business partners and/or its customers.

Figure 1: Information Asset Classification Matrix - based on the [National Institute of Standards and Technology \(NIST\) Federal Information Processing Standards \(FIPS\) Publication 199 – Standards for Security Categorization of Federal Information and Information Systems](#)

The information classification process must include the following:

1. Identifying information assets
2. Classifying information assets by confidentiality, integrity, and availability (CIA)
3. Determining controls based upon the classification

Identification of Information Assets

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

1. Grouping of Information Assets
2. Determining the information owner
3. Determining the information custodian
4. Identifying information assets

1. Grouping of Information Assets

In order 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 the high 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.

2. Determining the Information Owner

Responsibility for the classification and control of 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 and 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 improper access.

3. 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-State entity). 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. An information custodian may also be the information owner.

4. Identifying Information Assets

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

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

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 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" (i.e., HML).

Questions are categorized by confidentiality, integrity, and availability. If it is determined after answering a question that the rating for a security principle (e.g., confidentiality) is high, you are not required to complete the remaining questions in that category. However, doing so may provide you with a better understanding of the risks associated with the information asset. To save time, the questions at the beginning will typically help in determining whether the rating is high. Each question must be answered sequentially, to the best of the information owners' abilities.

Determination of Controls

Once the information is classified, the classification can be used to determine appropriate controls. At a minimum, baseline controls must be implemented. These controls, based on Federal guidance, industry best practice and classification of the information assets, are found in the [NYS Information Security Control Standard](#). SE's are required to augment these controls as necessary, using risk assessments and the security control baselines in [NIST Special Publication 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations](#).

5.0 Compliance

This standard shall take effect upon publication. The Policy Unit shall review the standard at least once every year to ensure relevancy. The Office may also assess agency compliance with this policy. To accomplish this assessment, ITS may issue, from time to time, requests for information to covered agencies, which will be used to develop any reporting requirements as

may be requested by the NYS Chief Information Officer, the Executive Chamber or Legislative entities.

If compliance with this policy 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 Enterprise Information Security Office exception process.

6.0 Definitions of Key Terms

Not applicable

7.0 ITS Contact Information

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

Standard Owner
Attention: Enterprise Information Security Office
New York State Office of Information Technology Services
State Capitol, ESP, P.O. Box 2062
Albany, NY 12220
Telephone: (518) 242-5200
Facsimile: (518) 322-4976

Questions may also be directed to your ITS Customer Relations Manager at:
Customer.Relations@its.ny.gov

The State of New York Enterprise IT Policies may be found at the following website:
<http://www.its.ny.gov/tables/technologypolicyindex.htm>

8.0 Review Schedule and Revision History

Date	Description of Change	Reviewer
10/10/2008	Original Standard Release (<i>released under the Office of Cyber Security and Critical Infrastructure Coordination (CSCIC)</i>)	
1/17/2014	Rebranded for the Office of Information Technology Services; (<i>replaces CSCIC/OCS PS08-001 Information Classification and Control</i>); 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
1/17/2015	Scheduled Standard Review	Deborah A. Snyder, Acting Chief Information Security Officer

9.0 Related Documents

- [Federal Information Processing Standards Publication 199: Standards for Security Categorization of Federal Information and Information Systems](#)
- [New York State Information Security Controls Standard](#)
- [New York State Risk Management Standard](#)

INFORMATION ASSET CLASSIFICATION WORKSHEET
CIA QUESTIONS

Appendix A

CONFIDENTIALITY QUESTIONS	INTEGRITY QUESTIONS	AVAILABILITY QUESTIONS
<p>1 Does the information include or contain PPSI (Personal, Private, or Sensitive Information)?</p> <p>A) No - continue with Confidentiality questions D) Yes - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>1 Does the information include medical records?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>1 Is availability of the information essential for emergency response or disaster recovery?</p> <p>A) No - continue with Availability questions D) Yes - Availability is High (rate below)</p>
<p>2 What impact does unauthorized access or disclosure of information have on health and safety?</p> <p>A) None - continue with Confidentiality questions B) Limited impact - continue with Confidentiality questions C) Serious impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>2 Is the information (e.g., security logs) relied upon to make critical security decisions ?</p> <p>A) No - continue with Integrity questions D) Yes - Integrity is High (rate below), continue with Availability questions</p>	<p>2 This information needs to be provided or available:</p> <p>A) As time permits - continue with Availability questions C) Within 1 to 7 days - continue with Availability questions D) 24 hrs. per day/7 days a week - Availability is High (rate below)</p>
<p>3 What is the financial impact of unauthorized access or disclosure of information?</p> <p>A) None - continue with Confidentiality questions B) Limited impact - continue with Confidentiality questions C) Serious impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>3 What impact does unauthorized modification or destruction of information have on health and safety?</p> <p>A) None - continue with Integrity questions B) Limited impact - continue with Integrity questions C) Serious impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>3 What is the impact to health and safety if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Limited impact - continue with Availability questions C) Serious impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>4 What impact does unauthorized access or disclosure of information have on the SE mission?</p> <p>A) None - continue with Confidentiality questions B) Limited impact - continue with Confidentiality questions C) Serious impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>4 What is the financial impact of unauthorized modification or destruction of information?</p> <p>A) None - continue with Integrity questions B) Limited impact - continue with Integrity questions C) Serious impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>4 What is the financial impact if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Limited impact - continue with Availability questions C) Serious impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>5 What impact does unauthorized access or disclosure of information have on the public trust?</p> <p>A) None - continue with Confidentiality questions B) Limited impact - continue with Confidentiality questions C) Serious impact - continue with Confidentiality questions D) Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>5 What impact does unauthorized modification or destruction of information have on the SE mission?</p> <p>A) None - continue with Integrity questions B) Limited impact - continue with Integrity questions C) Serious impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>5 What is the impact to the SE mission if information were not available when needed?</p> <p>A) None - continue with Availability questions B) Limited impact - continue with Availability questions C) Serious impact - continue with Availability questions D) Severe impact - Availability is High (rate below)</p>
<p>6 Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or disclosure of information.</p> <p>A) No - continue with Confidentiality questions B) Yes - Limited impact - continue with Confidentiality questions C) Yes - Serious impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>6 What impact does unauthorized modification or destruction of information have on the public trust?</p> <p>A) None - continue with Integrity questions B) Limited impact - continue with Integrity questions C) Serious impact - continue with Integrity questions D) Severe impact - Integrity is High (rate below), continue with Availability questions</p>	<p>6 What is the impact to the public trust if the information were not available when needed?</p> <p>A) None - see Instructions below B) Limited impact - see Instructions below C) Serious impact - see Instructions below D) Severe impact - Availability is High (rate below)</p>
<p>7 Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure.</p> <p>A) No - continue with Confidentiality questions B) Yes - Limited impact - continue with Confidentiality questions C) Yes - Serious impact - continue with Confidentiality questions D) Yes - Severe impact - Confidentiality is High (rate below), continue with Integrity questions</p>	<p>7 Is integrity addressed by law or regulation? If yes, determine the impact of unauthorized modification or destruction of information.</p> <p>A) No - continue with Integrity questions B) Yes - Limited impact - continue with Integrity questions C) Yes - Serious impact - continue with Integrity questions D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	
<p>8 Is the information publicly available?</p> <p>A) No - see Instructions below, then continue with Integrity questions B) Yes - see Instructions below, then continue with Integrity questions</p>	<p>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 information.</p> <p>A) No - see Instructions below then continue with Availability questions B) Yes - Limited impact - see Instructions below then continue with Availability ques. C) Yes - Serious impact - see Instructions below then continue with Availability ques. D) Yes - Severe impact - Integrity is High (rate below), continue with Availability ques.</p>	
<p>INSTRUCTIONS FOR RATING EACH COLUMN: If ALL of the above answers are A/B (GREEN), rating is LOW; if ANY of the above answers are C (YELLOW) and NONE are D (RED), rating is MODERATE; if ANY of the above answers are D (RED), rating is HIGH SCALE: A/B = GREEN = LOW C = YELLOW = MODERATE D = RED = HIGH</p>		

CLASSIFICATION RATING FOR CONFIDENTIALITY:

CLASSIFICATION RATING FOR INTEGRITY:

CLASSIFICATION RATING FOR AVAILABILITY:

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

Please note the information classification process described in this Standard is available in an automated tool called the Information Asset Classification System (IACS). This application is available to all New York State governmental entities utilizing NYS Directory Services. For further information, contact the Enterprise Information Security Office (EISO) at (518) 242-5200 or eiso@its.ny.gov.

Introduction

The classification of information will be the basis for many information security decisions in an organization. Before deciding the level of resources (i.e., 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 (i.e., 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 [Appendix C](#) 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

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

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 Information Portability and Accountability Act (HIPAA)).
- Retention requirements for the information asset.

Access Requirements:

- Who has/should have access to the information (i.e., 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 non-tangible assets of the State Entity such as reputation, trust and morale.

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

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**, contained in [Appendix A](#) contains the minimum questions that must be answered when classifying information. Following are example answers to assist in determining the appropriate response.

Confidentiality Questions

[1] 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 confidentiality of high. See the [NYS Information Technology Policies, Standards and Best Practice Guidelines Glossary](#) for a definition of PPSI.

[2] What impact does unauthorized access or disclosure of information have on health and safety?

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

[3] What is the financial impact of unauthorized access or disclosure of information?

Example(s): The State Entity may be exposed to litigation or regulatory fines due to disclosure of information protected by confidentiality agreements. For instance, unauthorized release of vendor bid information before the final submission date could jeopardize the bidding process leading to litigation.

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

[4] What impact does unauthorized access or disclosure of information have on the State Entity mission?

Example(s): An agency may be charged with ensuring that illegal goods do not enter State borders. As part of that mission, the agency may be responsible for collecting 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 agency's ability to conduct 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.

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

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

[5] What impact does unauthorized access or disclosure of information have on the public trust?

Example(s): It is important for the government to maintain the public's trust. Any breach of confidentiality that violates the public trust would typically lead to a severe impact for the State Entity. For example, the exposure of confidential medical records via a security breach could lead to a loss of public trust.

A department which collects and maintains the confidential records of citizens requires a high level of trust from the public. Disclosure of data through a malicious insider, external hacker, or through a random accident could erode trust leading to political consequences for department management and for the State as a whole.

[6] Is confidentiality mandated by law or regulation? If yes, determine the impact of unauthorized access or 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. 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.

[7] Is the information intended for limited distribution? If yes, determine the impact of unauthorized access or disclosure of 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.

[8] 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 any information that does not need to be withheld for security or privacy concerns is generally public. Examples include public transportation schedules, a listing of local city events and health improvement guidelines. These items would be ranked 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

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

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 alteration to such records in medical institutions can cause serious health consequences for the patients. Medical records require high integrity.

[2] Is the information (e.g., security logs) 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 records require high integrity.

[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 other information provided by surveillance.

Something that could be of limited to no impact on health and safety would be the modification of employee 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 indicate 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 the unauthorized modification or destruction of information have on the State Entity 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

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

was inaccurately modified without authorization and then posted to a public web site, the public would no longer trust the posting State Entity 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 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 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] Is availability of the information essential for emergency response or disaster recovery?

Example(s): If the information asset is required for emergency response, it could be essential in saving lives or in coordinating law enforcement and health officials during an emergency or disaster. Therefore, it must be available upon immediate request (high availability).

Disaster Recovery Plans need to be available in case of emergencies. Although required infrequently, they have a high availability status.

[2] 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.

[3] 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

APPENDIX B: INFORMATION CLASSIFICATION SUPPLEMENTAL GUIDANCE

availability to this data during emergency medical care can lead to life threatening situations therefore placing these items in the high availability category.

[4] 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.

[5] What is the impact to the State Entity 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.

[6] 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 are seriously degraded or disrupted, this could cause serious embarrassment to the State Entity resulting in a severe impact. The availability in this case would be high.

Determination of Controls

Once the information is classified, a listing of baseline controls for each type of classification can be found in the control charts in Appendix A of the [Information Security Controls Standard](#).

An electronic version of Appendix A of the Information Security Controls Standard is provided in an Excel format with the following features:

- all 27 classification ratings are hyperlinked to the appropriate control chart;
- each control in the control charts is hyperlinked to the appropriate entry in the Glossary of Information Security Controls; and
- the ALT + LEFT ARROW keys can be used to return to a previous page for ease of navigation in the spreadsheet.

Closing

Information classification is a necessary part of information security management in an organization. The purpose of this supplement has been to facilitate the implementation of information classification.

For information asset identification, a template has been provided to collect relevant pieces of information to assist in classification. Information asset classification has been simplified by the use of a structured questionnaire. Information owners answer a series of questions until they conclusively determine the classification level. This supplement also provides examples for each of the classification questions.

INFORMATION ASSET IDENTIFICATION WORKSHEET

Completed By:	
Completed Date:	
Department:	
Name of Information Asset:	
Information Asset Description/Comment:	
Information Asset Use: <small>(What business need does the information asset satisfy?)</small>	
Information Asset Format: <small>(i.e., paper, electronic)</small>	
Information Asset Storage: <small>(e.g., file cabinet, safe, database, network share, CD/DVD, portable drive)</small>	
Source of Information:	
Business Process(es) Supported:	
Information Owner:	
Information Custodian:	
Internal Information User(s):	
External Information User(s): <small>(e.g., other State Agencies, other governmental agencies, public)</small>	
Information Asset ID Number:	

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.