NATIONAL DATA
MANAGEMENT AUTHORITY

Information Classification Standard

Prepared By:

National Data Management Authority
March 2023

Document Status Sheet

	Signature	Date
Policy Coordinator (Cybersecurity)	**Muriana McPherson**	**31-03-2023**
General Manager (NDMA)	**Christopher Deen**	**31-03-2023**

Document History and Version Control

Date	Version	Description	Authorised By	Approved By
31-03-2023	**1.0**		**General Manager, NDMA**	**National ICT Advisor**

Summary

1. These standard addresses information classification.
2. It was adapted from NIST Cybersecurity Framework Policy Template Guide and SANS Institute.
3. This is a living document which will be updated annually or as required.
4. Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

1.0 Purpose

This standard outlines a classification process and provides procedures for classifying information in a manner that uniformly protects information entrusted to the organisation.

The process of classifying information pursuant to this standard may serve as a basis for an organisation 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 organisation.

2.0 Authority

The Permanent Secretary, Administrative Head, Head of Human Resources or their designated representative of the Public Sector Organisation is responsible for the implementation of this standard. For further information regarding the foregoing, please contact the Policy Coordinator - National Data Management Authority (NDMA).

3.0 Scope

This standard encompasses all systems, automated and manual, for which the Government of Guyana has administrative responsibility, including systems managed or hosted by third parties on behalf of the Government. It addresses all information, regardless of the form or format, which is created or used in support of business activities. It is the user's responsibility to read and understand this standard and to conduct their activities in accordance with its terms.

4.0 Standard

As per the Information Security Policy, all information and/or information systems must be classified. Information classification is based on three principles of security: confidentiality, integrity, and availability.

For each principle, information can be classified as low, moderate, or high. When classifying the impact, the organisation 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.

Table 1: The table below highlights the potential impact levels that the loss of confidentiality, integrity, or availability could have on an organisation.

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 organisational operations, organisational 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 organisation is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organisational 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 organisational operations, organisational 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 organisation is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organisational 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 organisational operations, organisational 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 organisation is not able to perform one or more of its primary functions; (ii) result in major damage to organisational 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.

Each organisation should review the impact levels in the context of its own operational environment.

Table 2 shows the Information Asset Classification Categories.

	INFORMATION CLASSIFICATION CATEGORIES per FIPS 199,		
	LOW	**MODERATE**	**HIGH**
CONFIDENTIALITY Consider impact of unauthorised disclosure on factors such as: 1.Health and Safety 2.Financial Loss 3. Organisation's Mission 4.Public Trust	The unauthorised disclosure of information could be expected to have **limited or no impact** on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **serious impact** on organisational operations, organisational assets, or individuals.	The unauthorised disclosure of information could be expected to have a **severe** or **catastrophic impact** on organisational operations, organisational assets, or individuals.
INTEGRITY Consider impact of unauthorised modification or destruction on factors such as: 5.Health and Safety 6.Financial Loss 7.Organisation's Mission 8.Public Trust	The unauthorised modification or destruction of information could be expected to have limited or **no impact** on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **serious impact** on organisational operations, organisational assets, or individuals.	The unauthorised modification or destruction of information could be expected to have a **severe** or **catastrophic impact** on organisational operations, organisational assets, or individuals.
AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as: 9.Health and Safety 10. Financial Loss 11. Organisation's Mission ▪ 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 organisational operations, organisational 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 organisational operations, organisational 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 organisational operations, organisational assets, or individuals.

Table 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[1]

[1] Retrieved from: NIST Computer Security Resource Center | CSRC
https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

4.1 Information Classification Process

The information classification process must include the following:

4.1.1 Identification of information assets;

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

4.1.3 Determining controls based upon the classification.

4.2 Identification of Information Assets

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

4.2.1 Grouping of information assets

4.2.2 Determining the information owner

4.2.3 Determining the information custodian

4.2.4 Identifying information assets

4.3 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 require 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 entity evaluates the risk and cost benefit of grouping a given set of assets.

4.4 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.

4.5 Determining the Information Custodian

Information custodians are people, units, or organisations responsible for implementing the authorised 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 organisation or from third parties (e.g., another entity). If the custodian is a third party, a formal, written agreement between the custodian's organisation and the entity that owns the information must specify the responsibilities of each party. An information custodian may also be the information owner.

4.6 Identifying Information Assets

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

4.6.1 Source of the information asset (e.g., unit, agency)

4.6.2 Use of the information asset (i.e., purpose/business function)

4.6.3 Business processes dependent on the information asset

4.6.4 Users/groups of users of the information asset

4.7 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 a Legal Counsel 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. An entity 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" (i.e., HML).

Questions are categorised 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 organisational policies and standards. Failure to comply with the standard may, at the full discretion of the Permanent Secretary, Administrative Head, or Head of Human Resources of the Public Sector Organisation, may result in the suspension of any or all privileges and further action may be taken by the Ministry of Public Service.

6.0 Exceptions

Requests for exceptions to this standard shall be reviewed by the Permanent Secretary, Administrative Head, Head of Human Resources of the Public Sector Organisation, or the Policy Coordinator, NDMA. Departments requesting exceptions shall provide written requests to the relevant personnel. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein.

7.0 Maintenance

The Policy Coordinator, NDMA shall be responsible for the maintenance of this standard.

8.0 Definitions of Key Terms

Term	Definition
User[2]	Individual or (system) process authorized to access an information system.
Confidentiality[3]	The term 'confidentiality' means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
Integrity[4]	The term 'integrity' means guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

[2]Retrieved from: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/user
[3]Retrieved from: NIST Information Technology Laboratory Computer Security Resource Center - https://csrc.nist.gov/glossary/term/confidentiality
[4] Retrieved from: NIST Information Technology Laboratory Computer Security Resource Center - https://csrc.nist.gov/glossary/term/integrity

Availability[5]	The term 'availability' means ensuring timely and reliable access to and use of information.
Information[6]	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. An instance of an information type.

9.0 Contact Information

Submit all inquiries and requests for future enhancements to the Policy Coordinator, NDMA.

[5] Retrieved from: NIST Information Technology Laboratory Computer Security Resource Center - https://csrc.nist.gov/glossary/term/availability

[6] *Retrieved from*: NIST Information Technology Laboratory Computer Security Resource Center https://csrc.nist.gov/glossary/term/information

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, public/private cloud storage) _____

Source of Information: _____

Business Process(es) Supported: _____

Information Owner: _____

Information Custodian: _____

Internal Information User(s): _____

External Information User(s): (e.g., other 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 unauthorised disclosure of information have on health and personal safety?				
4. What is the financial or agency liability impact of unauthorised disclosure of information?				
5. What impact does unauthorised release of sensitive information have on the entity mission?				
6. What impact does unauthorised 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 unauthorised 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 unauthorised 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				
	No		Yes	
1. Does the information include medical records				
	No		Yes	
2. Is the information (e.g., security logs) relied upon to make critical security decisions?				
	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 Organisation's 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 Organisation's 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 organisation. 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 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 familiarise 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 information.
- 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/entities, third-parties, governments.

Health and Safety Concerns:

- Impact on employees as well as the public.

Mission:

- The overall mission of the 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 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 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 personally identifying information (PII)?

   Example(s): A form that contains a name, as well as a National Identity 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.

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 entity's workforce and 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 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 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 organization to litigation. Similarly, if the investment decisions of the entity'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 unauthorised release of sensitive information have on the entity mission?

   Example(s): An entity may be charged with ensuring that illegal goods do not enter. As part of that mission, the entity 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, it could have a severe impact on the entity'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 unauthorised disclosure of information have on the entity'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 unauthorised exposure of medical records could lead to a loss of the public trust in the entity's ability to protect sensitive information.

   An entity which collects and maintains the confidential records of citizens requires a high level of public trust. Unauthorised 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 Organisation's Mission and their ability to protect citizen data.

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

   Example(s): Some types of information, including personal health records, student grades, and financial and personnel records may be protected by laws or regulations. Disclosing this information can lead to civil or criminal liability. There are several key statutes 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 unauthorised disclosure of that information.

   Example(s): Some information generated within an 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 an entity's assets, would require high confidentiality controls.

   Administrative information, such as procedures for travel approval, though not publicised outside the 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 unauthorised 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 unauthorised modification of an employee's calendars.

4. What is the financial impact of unauthorised 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 an 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 unauthorised modification or destruction of information have on the entity mission?

   Example(s): 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's 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 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 laws. Allowing unauthorized changes to information may have legal consequences. There may be several key legislations that should be examined based on the information asset being classified.

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 an 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 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 analysed and escalated based on the level of threat. Since security is critical, and severe damage can be caused to 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 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 entity mission if information were not available when needed?

   Example(s): Airline missions are to get customers safely and conveniently to various destinations. If access to airline schedules was unavailable, this could lead to an inability of the airline 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): 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 entity resulting in a severe impact and an erosion of the public's trust in the entity and the online services. The availability in this case would be high.