PROCEDURE: DATA CLASSIFICATION AND HANDLING

1.0 PURPOSE

Classification of data is a critical element of any mature information security program and fundamental to securing Hamilton College information assets. This procedure has been developed to assist, provide direction to and govern all entities of the organization regarding identification, classification and handling of information assets.

2.0 PROCEDURE

STEP 1 – IDENTIFY DATA ASSET

Identification of information assets involves creating an inventory of all information assets in the organization.

In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group information assets together. It is important to establish that the grouping of assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the information asset must be classified at the highest level necessitated by its individual data elements. For example, if Human Resources 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 controls for a confidentiality of HIGH.

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 a system (e.g., database, data warehouse, application server), it may be easier to apply controls if the system is classified as a single entity. However, costs may be reduced by applying the controls to the individual elements (e.g., field, record, application). Therefore, it is important that the organization evaluate the difference between the two to identify the most appropriate solution when determining the grouping of information assets for classification.

Examples:

Data Asset Name	Data Asset Owner	Confidentiality	Integrity	Availability
Student Grades				
Payroll Records				
(Institutional) Research Data				
Health Records				
Annual Report				
Admissions Data				
Campus Maps				

STEP 2 – IDENTIFY DATA ASSET OWNER

It is important to place the responsibility for the classification and control of an information asset with an individual or role. This should be an individual in a managerial position. If multiple individuals are found to be "owners" of the same information asset, an individual owner should be designated by a higher level of management.

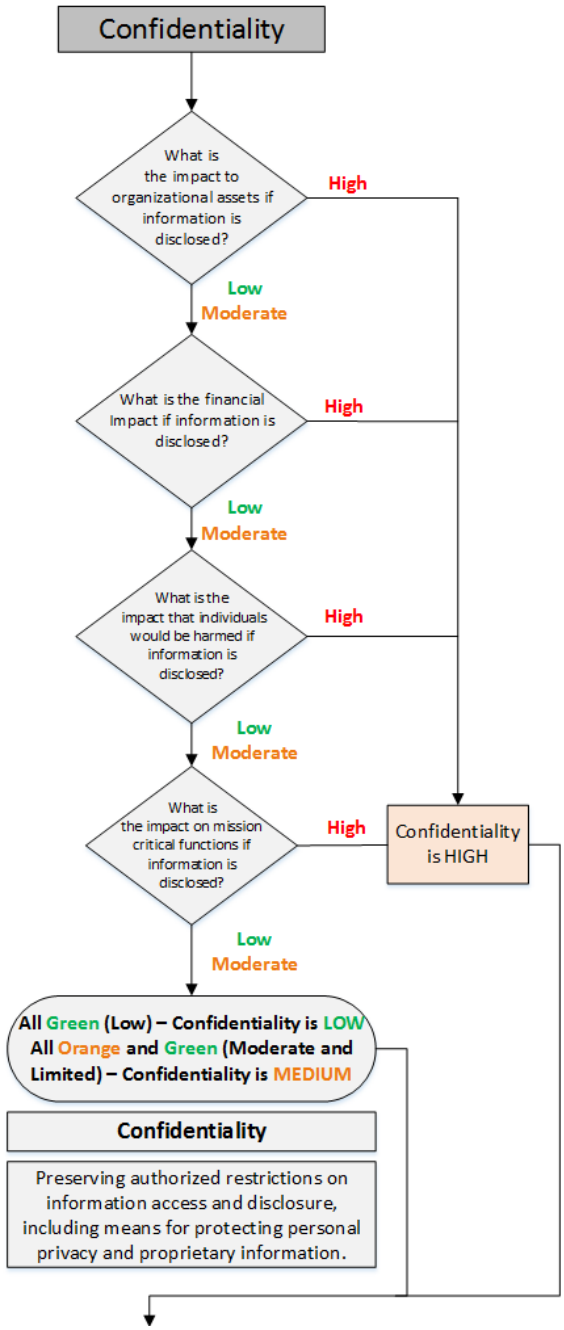
The information owner is responsible for determining the information's classification and how and by whom the information will be used.

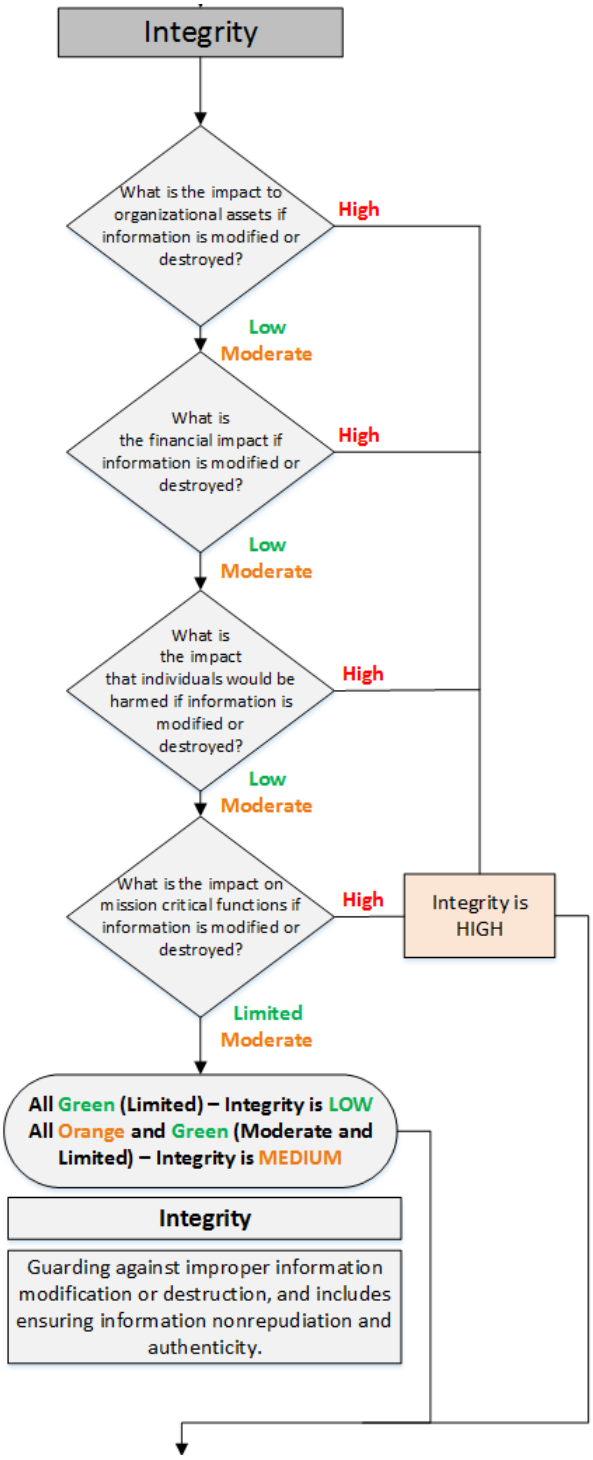
Examples:

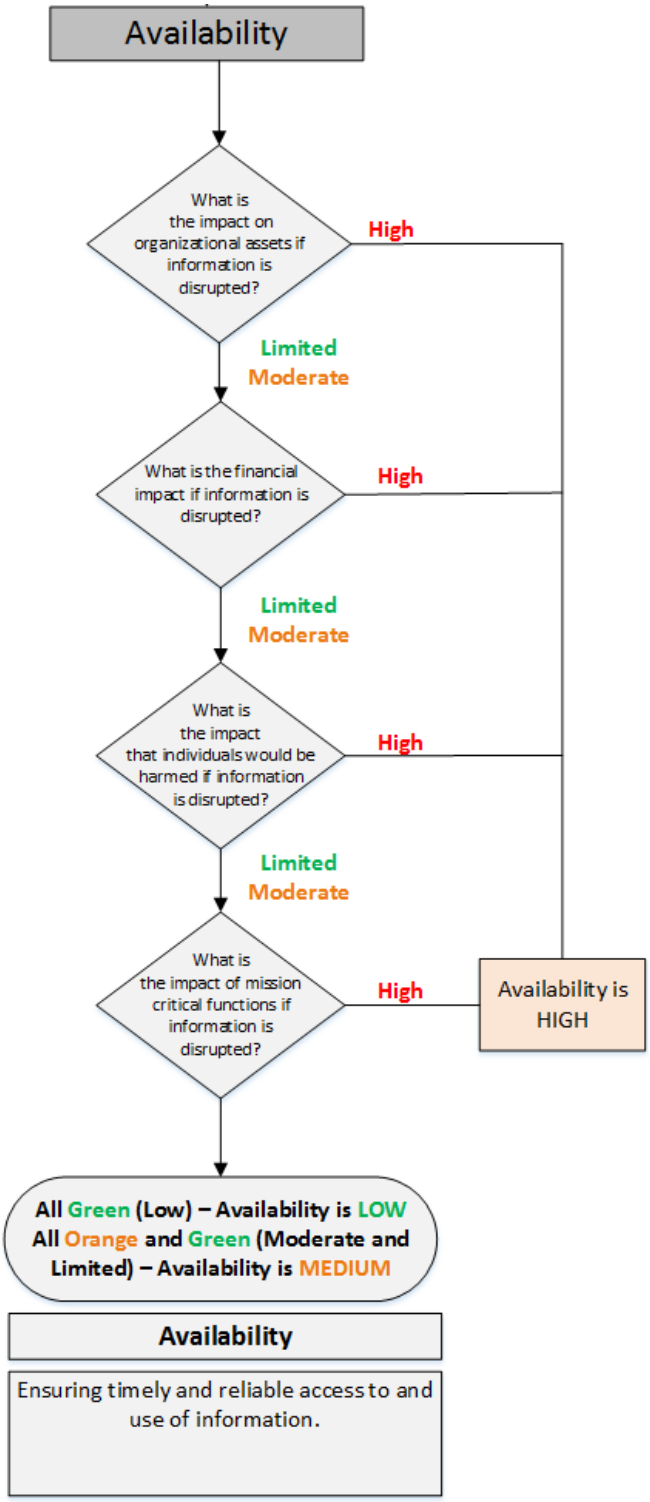
Data Asset Name	Data Asset Owner	Confidentiality	Integrity	Availability
Student Grades	Registrar			
Payroll Records	Controller and Director of Budgets			
(Institutional) Research Data	Institutional Research			
Health Records	Health Director			
Annual Report	Board of Trustees			
Admissions Data	VP of Admission			
Campus Maps	Campus Safety			

STEP 3 – EVALUATE DATA ASSET

Use the flowchart below to identify the levels for classification for the confidentiality, integrity and availability of each information asset. Classification of data will be based on specific, finite criteria as identified in the *Federal Information Processing Standard Publication 199 (FIPS-199).* Please see Appendix A for details on FIPS-199 categories.




Integrity
What is the impact to organizational assets if information is modified or destroyed?
High
Low
Moderate
What is the financial impact if information is modified or destroyed?
High
Low
Moderate
What is the impact that individuals would be harmed if information is modified or destroyed?
High
Low
Moderate
What is the impact on mission critical functions if information is modified or destroyed?
High
Integrity is HIGH
Limited
Moderate
All Green (Limited) – Integrity is LOW
All Orange and Green (Moderate and Limited) – Integrity is MEDIUM
Integrity
Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.


Availability
What is the impact on organizational assets if information is disrupted?
High
Limited
Moderate
What is the financial impact if information is disrupted?
High
Limited
Moderate
What is the impact that individuals would be harmed if information is disrupted?
High
Limited
Moderate
What is the impact of mission critical functions if information is disrupted?
High
Availability is HIGH
All Green (Low) – Availability is LOW
All Orange and Green (Moderate and Limited) – Availability is MEDIUM
Availability
Ensuring timely and reliable access to and use of information.

Examples:

Data Asset Name	Data Asset Owner	Confidentiality	Integrity	Availability
Student Grades	Registrar	High	High	High
Payroll Records	Controller and Director of Budgets	High	High	High
(Institutional) Research Data	Institutional Research	Moderate	Moderate	Moderate
Health Records	Health Director	High	Moderate	Moderate
Annual Report	Board of Trustees	Low	Low	Low
Admissions Data	VP of Admission	High	Moderate	Moderate
Campus Maps	Campus Safety	Low	Low	Low

STEP 4 – ASSIGN DATA CLASSIFICATION

The classification of a data asset will consist of all three categories (Confidentiality, Integrity and Availability) and will be in accordance with the FIPS199 standard. The classification can be against a data type and/or an entire information system (i.e. a Social Security number or the entire Colleague System.

Examples – (excerpts from FIPS 199):

Security Categorization Applied to Information TypesThe generalized format for expressing the security category, SC, of an information type is:

SC information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

where the acceptable values for potential impact are LOW, MODERATE, HIGH, or NOT APPLICABLE. (N/A only applies to the security category of Confidentiality – not integrity or availability).

Example 1 - Classifying a social security number:

SC (SSN) = {(**confidentiality**, High), (**integrity**, High), (**availability**, MODERATE)}

Security Categorization Applied to Information Systems

The generalized format for expressing the security category, SC, of an information system is:

SC information system = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)},

Note that the value of *not applicable* cannot be assigned to any security objective in the context of establishing a security category for an information system. This is in recognition that there is a low minimum potential impact (i.e., low water mark) on the loss of confidentiality, integrity, and availability for an information system due to the fundamental requirement to protect the system-level processing functions and information critical to the operation of the information system.

Example 2 – Classifying an information system (The Colleague system which contains information types ranging from Low to High).

SC (Colleague public directory info) = {(**confidentiality**, N/A), (**integrity**, MODERATE), (**availability**, LOW)}

AND

SC (Financial Data) = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

The resulting security category of the **information system** is expressed as:

SC (Colleague system) = {(**confidentiality**, HIGH), (**integrity**, HIGH), (**availability**, HIGH)}

representing the high water mark or maximum potential impact values for each security objective from the information types resident on the Colleague system.

STEP 5 – IMPLEMENT DATA HANDLING CONTROLS

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods, among others.

In general, controls assigned by Data Asset Owners will deal with the confidentiality category of the data. The categories representing Integrity and Availability will be used to guide the approaches taken by Hamilton College to protect against the loss or corruption of the data (usually at the system level by LITS personnell).

The control for each classification category (C,I,A) should be considered with respect to the corresponding rating. The following is a partial list of controls to be applied to data assets, based on their classification.

DATA HANDLING CONTROLS

Controls Key C=Confidentiality I=Integrity A=Availability	High	Moderate	Low	Prohibited
Access (C)	• Strong password(s) • Access request, review, approval and termination process • Asset Owner-approved access • Non-Disclosure Agreement (NDA) for third-parties • Immediate retrieval when printing or faxing • Secure storage when not in use • Situational awareness for verbal communications	• Password(s) • Access request, review, approval and termination process • Secure storage when not in use • Situational awareness for verbal communications	• Access request, review, approval and termination process	• N/A
Encryption (C,I)	• Encryption during creation, storage, processing and transmission • Encryption for third parties	• Encryption during transmission • Encryption for third parties	• None	• N/A
Labelling (C,I)	• Document watermark	• None	• None	• N/A
Monitoring (I,A)	• Security and availability	• None	• None	• N/A

Controls Key C=Confidentiality I=Integrity A=Availability	High	Moderate	Low	Prohibited
	monitoring and alerting • Privileged identity monitoring			
Retention **(I,A)**	• Backup testing and verification • Inclusion in Business Continuity and Disaster Recovery Plans • Redundancy or automatic failover • Offsite backup • Secure physical storage	• Backup testing and verification • Inclusion in Business Continuity and Disaster Recovery Plans	• None	• N/A
Destruction **(C)**	• Secure destruction, including shredding and secure wiping	• Secure destruction, including shredding and secure wiping	• None	• N/A
Audit **(I)**	• Annual controls audit	• Biennial controls audit	• None	• N/A
Physical **(C,I,A)**	• Secure courier when shipping • Media possession at all times • Lock/logout workstaions • Servers hosted in secure data centers	• Lock/logout workstaions • Servers hosted in secure data centers •	• None	• N/A
Backup/Disaster Recovery **(I,A)**	• Server - Daily backups, replicas, and multiple copies of data in different locations • Workstations – CrashPlan backup	• Server - Daily backups and multiple copies of data in different locations • Workstations – CrashPlan backup	• None	• N/A

APPENDIX A – FIPS 199 CATEGORIES

	INFORMATION CLASSIFICATION CATEGORIES		
	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 access or disclosure of information would have ***minimal 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 only ***limited 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 impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
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 would have ***minimal 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 only ***limited 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 impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
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 would have ***minimal 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 only ***limited 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 impact*** on the organization, its critical functions, workforce, business partners and/or its customers.