	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

## 1.0 PURPOSE

---

The purpose of this policy is to define the data classification requirements for information assets and to ensure that data is secured and handled according to its sensitivity and impact that theft, corruption, loss, or exposure would have on the institution. This policy has been developed to assist Aurora University and provide directions to the institution regarding identification, classification, and handling of information assets.

## 2.0 SCOPE

---


The scope of this policy includes all information assets governed by Aurora University. All personnel and third parties who have access to or utilize information assets to process, store and/or transmit information for or on behalf of Aurora University shall be subject to these requirements.

## 3.0 ROLES AND RESPONSIBILITY

---

The scope of this policy includes all information assets governed by Aurora University. All personnel and third parties who have access to or utilize information assets to process, store and/or transmit information for or on behalf of Aurora University shall be subject to these requirements.

- Information Technology Service Team – Responsible for creating and managing asset inventories used to process, store, transmit, or provide access to electronic information. Information Technology Services is the custodian for this policy.
- Information Technology Services – Responsible for monitoring the implementation of this policy and reporting to Chief Information Officer on any abnormal findings or exceptions.
- Employees with access to PHI/ePHI, Student Information, PII –
  - Responsible for classifying by storing, in confidential location, all created or modified information, including any reproductions that are made (e.g., reports).
  - Responsible for appropriate handling of all classified information (electronic or non-electronic).

	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

- Data owners - individuals, roles, or committees primarily responsible for information assets. These individuals are responsible for:
  - Identifying the institution's information assets under their areas of supervision; and
  - Maintaining an accurate and complete inventory for data classification and handling purposes.
  - Communicate that information assets receive an initial classification upon creation.
  - Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified.
  - Reporting deficiencies in security controls to management.

## 4.0 POLICY

---


Aurora University has established the requirements enumerated below regarding the classification of data to protect the institution's information.

### 4.1 DATA CLASSIFICATION

---

Classification of data will be performed by the data asset owner based on the specific, finite criteria. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications will be defined as follows:

- **RESTRICTED** - Information whose loss, corruption, or unauthorized disclosure would cause **severe** personal, financial, or reputational harm to the institution, institution staff or the people we serve. Federal or state breach notification would be required, identity or financial fraud, extreme revenue loss, or the unavailability of extremely critical systems or services would occur. Common examples include, but are not limited to, social security numbers, banking and health information, payment card information and information systems' authentication data.
- **SENSITIVE or INTERNAL** - Information whose loss, corruption, or unauthorized disclosure would likely cause **limited** personal, financial, or reputational harm to the institution, institution staff or the people we serve. Federal or state breach notification would not be required, limited identity theft and very little revenue loss would occur, and the availability of critical systems would not be affected. Common examples include, but are not limited to, some data elements found in HR employment records, unpublished research data, and passport and visa numbers.

	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

- **PUBLIC** – Information whose loss, corruption, or unauthorized disclosure would cause **minimal or no** personal, financial, or reputational harm to the institution, institution staff or the people we serve. Common examples include, but are not limited to sales and marketing strategies, promotional information, published research data, and policies.

## 4.2 DIRECTORY INFORMATION

---

Workforce Information is defined as the following:

- Name
- Department of assignment, including office telephone/fax number, department email address

Workforce directory information is published on the Aurora University Intranet.

## 4.3 DATA HANDLING

---

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods. The specific methods must be described in REF03-Information Handling Guidelines.


## 4.4 LABELING

---

Information labeling is the practice of marking an information system or document with its appropriate classification levels that others know how to appropriately handle the information.

There are several methods for labeling information assets.

- **Printed/Emailed:** Restricted information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts).
- **Displayed:** **Restricted** or **Internal** information that is displayed or viewed (e.g., websites, presentations, etc.).
- Materials that will be utilized internally at Aurora University are expected to be handled in accordance with their classification based on the training provided to employees.

	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

#### 4.5 RE-CLASSIFICATION

---

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired, or destroyed.

#### 4.6 CLASSIFICATION INHERITANCE

---

Logical or physical assets that “contain” a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

#### 4.7 ACCESS

---

Information Stewards are responsible for ensuring all the workforce are provisioned with appropriate access to information and information systems. Access to information and information systems will be provisioned on a least privileged basis. Should additional access be required to perform job functions, reference the institution’s Access Control Procedure for steps on how to request additional access:

Access Control Procedure

#### 4.8 RETENTION & DESTRUCTION

---

Information will be retained in compliance with institution defined retention schedules:

Retention Schedule


Information will be destroyed in compliance with institution defined destruction procedures:

Information Destruction Procedure

#### 4.9 ASSET INVENTORY

---

See Asset Inventory matrix located here: [Asset Inventory and Information Classification](#).

	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

## 5.0 ENFORCEMENT

Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action both within and outside of the institution. The institution may temporarily suspend or block access to an account prior to the initiation or completion of such procedures, when it appears reasonably necessary to do so to protect the integrity, security or functionality of the institution or other computing resources or to protect the institution from liability.

## 6.0 EXCEPTIONS

Exceptions to this policy must be approved in advance by the Chief Information Officer, at the request of the data asset owner responsible. Approved exceptions must be reviewed and re-approved by the asset owner annually.

## 7.0 REFERENCES

- Federal Information Processing Standard Publication 199 (FIPS-199)
- NIST Special Publication 800-171

## 8.0 RELATED POLICIES


- Acceptable Use Policy
- Information Security Policy

## 9.0 RESPONSIBLE DEPARTMENT

Information Technology Services

## 10.0 REVISION HISTORY

Version	Date	Author	Revisions
1.0		GreyCastle Security	Original

	<i>Information Classification Policy</i>
Effective Date 5/5/2022	Version 1.3

1.1	8/18/2022	Aurora Team	Review, Approve, Publish
1.2	10/23/2023	CIO	Annual Review
1.3	8/22/2024	CIO	Annual Review

## 12.0 APPROVALS

Executive		Chief Information Officer	
Name		Name	
Jeff King		Hurstel Howard	
Title		Title	
COO		CIO	
Date		Date	
8/18/2022, 10/23/2023, 8/22/2024		8/18/2022, 10/23/2023, 8/22/2024	
Signature		Signature	
Jeff King		Hurstel Howard	