Elmhurst College

POLICY ON THE DEFINITION, CLASSIFICATION, STORAGE, AND USE OF SENSITIVE INFORMATION

1. Overview

Members of the Elmhurst College community are responsible for properly using and, when appropriate, protecting sensitive information that has been collected, produced or maintained by Elmhurst College in connection with its mission and/or operation. Sensitive information must be assigned a level of protection that is commensurate with the type of information and the purpose for which it was collected, obtained, or produced. Assigning the appropriate level of protection to sensitive information is called data classification.

Much of the information under Elmhurst College's control is classified as public information, in physical and/or electronic format, and can be shared without constraint. However, some information is classified as sensitive and non-public. Examples include personally identifiable information, Elmhurst College proprietary institutional information, other sensitive data, or information that is controlled by laws or regulations. Whether in physical and/or electronic format, data custodians must identify and appropriately classify sensitive information so it is protected appropriately. Members of the Elmhurst College community must know the difference between public information and sensitive information and how to classify and protect sensitive information.

2. Purpose

The purpose of this policy is to protect sensitive information within the Elmhurst College community from unauthorized access or disclosure. Every member of the community is obligated to protect sensitive information and should be aware of the four data classification levels used to identify and secure sensitive information. The goal is to assure that every member of our community can readily define sensitive information**,** such as Social Security Numbers (SSN), or financial data in conjunction with a person's name, so they can appropriately classify the information, follow appropriate security precautions to protect the information, and not jeopardize the privacy rights of others or Elmhurst College's institutional rights or obligations.

3. Scope

This definition applies to individuals accessing information, in physical or electronic format, obtained by or from Elmhurst College staff, faculty, students, contractors or visitors using Elmhurst College facilities, services or systems. All members of the Elmhurst College community who have access to information must understand these definitions and evaluate their actions consistent with Elmhurst College policies for safeguarding the privacy of information. All individuals who are data custodians as well as individuals accessing and using data are bound by this policy.

4. Policy

The data custodian must define the data classification level for any records he or she maintains in electronic or physical form based upon the data sensitivity. This

classification level will range from Level 0 (public) to Level 3 (access regulated by law or contract). As data classification levels increase from 0 to 3, more secure technical and procedural security requirements must be implemented. For research data, Elmhurst College follows the data classification scheme below unless the research sponsor has a specific data use agreement that proscribes specific data protection requirements. The data custodian is responsible for informing the Office of Information Services of any data classified above level 0 so that the appropriate protections can be established.

- **Level 3**.
  Information designated as sensitive by laws or regulations, such as
  - Medical records covered by the Health Information Portability and Accountability Act (HIPAA)
  - Banking and credit card records covered by the Payment Card Industry (PCI) data security standards.

  Information of this type is <u>always sensitive</u> if personal identifiers (e.g. name, SSN, Elmhurst College ID, etc.) are, or can be, associated with the medical or banking records. This type of sensitive information receives the highest level of security protection within Elmhurst College's systems and must never be extracted from those systems without express written permission from the appropriate Vice President.

- **Level 2**.
  Personally identifiable information collected and retained by Elmhurst College about any member or affiliate of the Elmhurst College community.
  This includes:
  - Any individual's first name or first initial and last name* in combination with one or more of the following data elements
    - SSN
    - Taxpayer Identification Number
    - Driver's License Number
    - Passport Number
    - Financial, Credit, or Debit Account Numbers
  - Any individual or combination of data elements that, if disclosed without authorization, identifies a specific individual and could place the individual's privacy, or Elmhurst College at risk.

  This type of sensitive information is also protected securely within Elmhurst College's systems and must be secured with the same level of protection if extracted from those systems.

- **Level 1**.
  Elmhurst College proprietary institutional information, including:
  - Academic records covered by the Federal Education Right and Privacy Act (FERPA);
  - Sensitive institutional information such as intellectual property, project proposals, or patent applications; and
  - Administrative Correspondence containing personally identifiable information or otherwise marked confidential due to its content.

  This type of sensitive information also is protected securely within Elmhurst College's systems and must be secured with the same level of protection if extracted from those systems.

- **Level 0**.
  Public Information not classified as level 1-3.

Appropriate Data Use

Members of the Elmhurst College community who use any of the services listed in Table 1 below must do so in accordance with the policies and guidelines that govern general technology use on campus. Users who have access privileges to any of Elmhurst College's systems must be aware of the sensitivity level of any data extracted from a central system that might later be stored using one of the methods listed in Table 1. Before doing so, users must ensure the security risk level of the storage target is consistent with the level of protection required for the extracted data and must obtain approval from a supervisor or manager for Level 2 data and higher. Contact OIS if there are questions about the use of sensitive information in any Elmhurst College system. Sensitive Information belonging to multiple sensitivity levels must be treated according to the highest level of sensitivity.

Table 1 Approved Risk Level by Storage Category or Device

Approved Risk Level

Service	0	1	2	3	Comments
Elmhurst College Owned Workstations	✓	✓			Level 0 and 1 data can be stored locally on your workstation. Level 2 data must be stored on OIS-approved secure centralized file shares or OIS-approved encrypted portable electronic storage devices. Level 3 data must be stored in ways explicitly designed and approved by OIS.
Personally Owned Workstations	✓				Personally owned workstations can only be used to store Level 0 data, that is, only Elmhurst College public information.
Active Directory-based Centralized File Share (Exablox)	✓	✓	✓		Work with OIS to establish an appropriate secure share for Level 2 data.
Office 365 - OneDrive	✓	✓			Consult with OIS before using Office 365 – OneDrive storage for any new purpose to ensure proper security settings for shared O365 files and sites.
Office 365 – OIS Designed Share or Site			✓		OIS must explicitly design any O365 environment used to store Level 2 data. O365 provides sufficiently robust security for Level 2 data when appropriately configured and managed.
Email	✓				Never send Level 1 or higher data through email regardless of the email provider. Use an approved Office 365 share or an Active Directory-based centralized file share to share Level 1 or Level 2 data.
Google Apps	✓				Google Apps may only be used to share Level 0 public data.
Mobile Devices	✓				Mobile devices, whether Elmhurst College or personally-owned, may be used only with public, Level 0, Elmhurst College information.

Service	0	1	2	3	Comments
Public Cloud Storage Sites (e.g. Dropbox)	✓				Public Cloud storage other than approved O365 accounts may be used only for public information.
Portable Electronic Storage Media	✓				Never store Level 1, 2 or 3 data on portable electronic storage media such as USB devices, CD/DVD ROM, or external hard drives.
Encrypted Portable or Local Electronic Storage Media	✓	✓	✓	✓	Work with OIS to design, acquire, and properly configure any encrypted portable or local storage environment. All storage for Level 3 data must be explicitly approved by the Chief Information Officer or his/her appointed designee.

5. Policy Compliance

Compliance Measurement

The Office of Information Services (OIS) will verify and promote compliance to this policy through various methods, including but not limited to, reports, internal and external audits, and feedback to individuals and campus departments.

Exceptions

Any exception to the policy must be approved by Chief Information Officer in advance.

Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5. Related Standards, Policies and Processes

- *Acceptable Use Policy*
- *Email Policy*
- *Password Policy*