Faculty/Staff Acceptable Use Policy

Glossary of Terms:

PII: Personally Identifiable information. For example Social Security Numbers, Date of Birth, home address.

Security Incident: Examples include opening an unknown email attachment, downloading an unknown file, clicking on a suspicious link, losing a company device, etc.

Encryption: The process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. Encryption does not itself prevent interference but denies the intelligible content to a would-be interceptor.

Data: Information stored in an electronic format.

Endicott owned information systems: All data systems owned and controlled by Endicott College or created on Endicott College owned property. Examples include but are not limited to emails, chat logs or text messages sent on or to Endicott college owned equipment or systems.

Purpose

The purpose of this policy is to outline the acceptable use of all technology and systems, including hardware, software and data at Endicott College (Endicott). This policy serves to protect both the employees and Endicott by helping to ensure the protection of information systems, including the confidentiality, integrity, and availability of Endicott data.

Scope

This policy applies to all Endicott Administration, Faculty, Staff, and any third parties, contractors, temporary or part-time employees, and any other personnel that have a legitimate need to access information systems owned or operated by Endicott College.

Roles and Responsibilities

President's Council - Responsible for making a final review and approval of this policy.

Chief Information Officer – Responsible for reviewing and approving this policy prior to President's Council. The CIO should report all relevant compliance-related activities pertaining to this policy to President's Council.

Human Resources – Responsible for ensuring all employees are made aware of this policy. Human Resources should maintain records of employee acknowledgement.

Information Technology: Responsible for training employees on any aspects of this policy where such is required.

Policy

Acceptable Use

All Endicott College technology systems are restricted to use for approved College purposes only and may be monitored for compliance with this acceptable use policy. Examples of acceptable use cases include:

- The use of Endicott College information systems for official purposes only. For example Using email for the functions of your job.
- All users of Endicott College systems must use only College approved and/or provided technology to access said systems, including on-site and remote access.
- All users of Endicott College may access, use, or share Endicott College proprietary information only to the extent it is authorized and necessary to fulfill assigned job duties.

Privileged User Access

Privileged users that have administrative privileges may only use their privileged user accounts for actions requiring elevated privileges. Privileged users must use their non-privileged user account when performing functions at a general user level, such as checking College email, internet access, or other general user functions.

Individual Accountability

All users accessing Endicott College systems and/or data are individually accountable for their actions. This includes but is not limited to:

- Printing – ensuring any printed documents are retrieved from printers and any unneeded/extra documents are securely shredded.
- Transmission of PII - All personally identifiable information should be handled with care. No PII should leave the college via unencrypted methods and only with specific approval to do so due to job function requirements.
- Transporting documents and data – when transporting documents and data within Endicott College facilities or off-site, ensuring they remain secure and are not left in unsecured areas.
- Email attachments – ensuring emails and attachments are only sent to the intended recipients and are encrypted when possible.

- Individual workstations – all users must lock their screen when away from their workspace.
- Passwords – should not be written down or saved in an insecure manner (i.e. outside a College approved password vault).
- Equipment assigned to individuals should be secured (i.e. don't leave equipment in uncontrolled/public areas). Note there are general use computers in classrooms and labs which are secured with tethered locks.

Unacceptable Use

Unacceptable use consists of any inappropriate and/or unnecessary use of Endicott College systems and data. All Endicott College stakeholders should use their best judgment in determining whether a specific use meets a College/business need. If there is any uncertainty as to the genuine College/business need for a specific use, an exception request should be submitted (see Exceptions section below). Examples of unacceptable use include, but are not limited to:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations.
- Using devices with no identifiable owner.
- Using of unapproved devices or media.
- Using of unapproved file transfer methods.
- Unauthorized use or sharing of Endicott College systems, assets, and data.
- Using personal email to conduct business where Endicott College email should be utilized.
- Using Endicott College email for personal business.
- Attempting to bypass any Endicott established security measures.
- Violating established policy, procedure, or processes related to information security and/or cybersecurity.
- Installation of unapproved software on Endicott College systems.
- Storing personal documents or photographs on Endicott devices.
- Sharing passwords to your Endicott accounts or any accounts you use in your work for Endicott.

Personal use of College Resources

Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Examples of personal use include but are not limited to:

- Using personal email accounts while at work.
- Using personal devices on the college network.
- Browsing the internet or checking social media from a work computer.

If there is any uncertainty, employees should consult their supervisor or manager.

Social Media

Use of Endicott College hardware resources to access social media should be limited. While now a regular part of some people's lives it poses risks for social engineering, malware distribution and data exfiltration.

Clear Desk

Employees are required to ensure that all sensitive/confidential information in electronic form or printed from an electronic system is secure in their work area when they are away from their work area. Computer workstations must be screen-locked or shut down when a workspace is unoccupied.

Security Incident Reporting

Security is a shared responsibility of all Endicott College stakeholders. If any Endicott College stakeholder has been potentially involved in, observed, or otherwise has knowledge of a security incident they are responsible for promptly

reporting the theft, loss, or unauthorized disclosure of Endicott College proprietary information to the proper Endicott personnel which can include both Campus Police and members of the Information technology department depending on the specific incident.

Policy Compliance

Endicott College reserves the right to audit College networks, systems, workstations, devices, etc.,on a periodic basis to ensure compliance with this policy. Computer processes may be used to monitor for improper transmission of data or suspicious activity.

Exceptions

Any exceptions to this policy must be requested and approved in writing. An exception request should be submitted by the employee's supervisor to Information Security for review and approval by the CIO

Disciplinary Action

Any personnel who fail to comply with this acceptable use policy or any other information security policies and procedures may be subject to disciplinary action up to and including termination of employment.

Access Control

Endicott owned information systems may be accessed and reviewed by Endicott information security personnel or their proxy as designated by the CIO for purposes of investigation. Investigations for purposes of Title IX or Handbook/AUP violations are limited to those requested by the head of Human Resources or Endicott counsel in writing to the CIO. These systems may also be accessed to investigate data security incidents, or upon initiation of a support request involving said systems.

After the termination of employment, accounts and systems of employees may be accessed by other employees for purposes of work continuity or for other business reasons . Email accounts may be forwarded for business continuity reasons at the discretion of the Area VP. Full access to accounts and systems themselves should be at the discretion of the Area VP with notification to the head of Human Resources.