I. Purpose

To establish the permitted and prohibited use of the College's information assets**.**

II. Scope

This policy applies to all LCC employees and covers all information assets, including computers and communication devices used, maintained, owned, and/or operated by the College as well as LCC-owned information stored on a remote system operated by an outside entity. This policy also covers any computer or communications device that is present on the College premises and/or uses the College communication infrastructure (which may not be owned or operated by the College).

III. General

A. Organization

1. The Information Security Management System will be modeled and evaluated after the National Institute of Standards and Technology Cybersecurity Framework standard and will use its process approach to understand the College's security requirements and to enact the needed monitoring and controls. A security strategy of Defense in Depth will be employed to manage the risk to information as required by the classification of the information. In addition, the College will protect its information assets in a legal and ethical manner and in accordance with good business practice.

2. Every LCC user is responsible for the use and protection of information assets within their functional responsibility. The LCC categories of responsibility for Information Security Managers are:

    a. **Owners** – All information assets must have an identifiable owner, either a manager or a non-manager representing management, who is responsible for identifying, classifying, authorizing access to, and protecting specific information assets.

    b. **Users** – Students, employees, Trustees, alumni, and contractors are responsible for using appropriate security to safeguard the information that they are authorized to access.

    c. **Contractors** – Service suppliers of hosting, telecommunications, data storage, or operations services have the responsibility for the safekeeping and operating functions, in accordance with security measures appropriate for the information assets over which they have custody. Information that is in the custody of the College and entrusted to an entity outside of the College by means of a contracted service or partnership must be afforded the same protection as similar LCC-owned information. LCC management will evaluate outside entities to determine the level of protection that the outside entity is expected to provide.

d. **Custodians - I**nformation technology professionals, engineers, and technical support staff responsible for the operation and management of systems and servers which collect, manage, and provide access to college data. Custodians are responsible for the protection and maintenance of information assets.

B. Classification of Information Assets

Information assets will be identified by the Information owners to classify the asset's value to the College. The Information Owner will identify the Information assets and will classify the information sensitivity as either public, private or confidential. The Information assets will also be classified based on availability, i.e., normal, essential, or critical. These classifications will be used by the College to determine the level of risk associated with the operation of each information resource.

1. **Sensitivity classifications~~:~~**

   a. **Public** – Information that is in the public domain or information intended to be communicated to the general public or community. This classification includes course descriptions or information about the services of the College.

   b. **Private** - Information that should not be available to a general population. This classification includes employee procedure manuals, department financial records, salaries, and date of birth.

   c. **Confidential** – This information needs to be safeguarded because of regulation or determination of the College that the loss of this information would cause devastating financial loss or loss of reputation. This classification includes most information about students and employees, academic, financial, or medical records.

2. **Availability classifications**

   a. **Normal** – Information assets that have a limited impact on the operations of the College as a whole or information that can be unavailable for up to a week or more.

   b. **Essential** – Information assets that are used to support operations of the College, but alternate resources can be used or a limited outage of a day or two is acceptable.

   c. **Critical** – Information assets that are required for the operation of the College divisional processes, both academic and administrative (for example: telephones and data network).

C. Risk Assessment and Risk Management

Risk Assessment of information assets is a formal process that will describe the risk of the occurrence of threats to LCC and the method chosen to mitigate the threat. This process will result in the creation of a document for review by management that describes the risks, the safeguards that will be employed, and the remediation

determined to best mitigate any threat or incident involving LCC information**.** The management of LCC can choose to:

1. **Accept the risk** – This alternative is taken if the probability of occurrence is very low or the cost of protective measures is too great. This alternative could also be used for low value or easily replaceable information, such as expendable supplies or public domain information.

2. **Transfer the risk** – This alternative is implemented through the use of contractual obligations, such as insurance.

3. **Reduce the risk** – This alternative is taken by installing protective measures or by establishing continuity plans.

D. Reviewing and Testing

The College will periodically assess through internal and external reviews if current practices provide the desired protection to achieve the intended security objectives. Owners, users, custodians, or suppliers of services of the College information assets must conduct reviews each year to assure compliance with the College Information Security Policy**.**

E. Destruction and Declassification of Media

The LCC Information Security Policy requires the destruction or declassification of information resources, including waste materials, which were used for recording confidential information when such information is no longer needed. Media that cannot be used again (e.g. paper) must be destroyed and media that can be used again (e.g. magnetic disks) must be either declassified or destroyed beyond recognition and reconstruction. Media declassification means that the critical information recorded on the media is destroyed usually by overwriting or degaussing. The quantity of critical information should be reduced to the minimum necessary.

F. Incident Response

The College's Information Security Policy requires the reporting of:

1. Incident of suspected or actual loss or compromise of LCC information, resource, or service.
2. Any violation or suspected violation of LCC Information Security Policy standards, procedures, or guidelines.

The requirements for incident reporting apply to all employees, students, contractors, and suppliers of LCC at all times. Such incidents must be reported whether they are intentional or unintentional to abuse@lcc.edu. See the LCC Incident and Response procedures for further requirements regarding incident reporting and response.

G. Education and Awareness

It is the responsibility of individual management, with the assistance of Information Security department, to ensure that all employees who use LCC information resources are adequately trained in security procedures and policy. It is the responsibility of the Information Security department to ensure that all students who use LCC information resources are adequately trained in security procedures and policies.

IV. Responsibility

Responsibility for the interpretation and administration of this policy is delegated to the Chief Information Officer or designee.

Adopted: 5/21/2007
Revised: 12/17/2018, 11/15/2021