Lehigh Carbon
COMMUNITY COLLEGE

Policy No. 3-235

SECTION 3: ADMINISTRATIVE REGULATIONS
2. Collegewide Regulations

TITLE: Technology – Cyber Security - Incident Response
ADOPTED: July 5, 2018 (Resolution 54.03)
REVISED: February 4, 2021 (Resolution 56.27)

Technology – Cyber Security - Incident Response

Purpose

It is the policy of the Lehigh Carbon Community College (“College”) to handle “information security incidents” so as to minimize their impact on the confidentiality, integrity, and availability of the College's systems, applications, and data. An effective approach to managing such incidents also limits the negative consequences to both the College and individuals, and improves the College's ability to promptly restore operations affected by such incidents.

It is especially important that serious information security incidents that may result in disruptions to important business processes are promptly communicated to the appropriate College officials so that they are involved early in decision-making and communications. In addition, compliance with various federal and state regulations requires expeditious reporting of certain types of incidents.

While information security incidents are not always preventable, appropriate procedures for incident detection, reporting and handling, combined with education and awareness of the College community, can minimize their frequency, severity, and potentially negative individual, operational, legal, reputational, and financial consequences.

Goals

The goals of establishing a successful incident management capability include:

1. Mitigating the impact of Information Technology (IT) security incidents.
2. Identifying the sources and underlying causes of IT security incidents and unauthorized disclosures to aid in reducing their future likelihood of occurrence.
3. Protecting, preserving, and making usable all information regarding the incident or disclosure as necessary for forensic analysis and notification.
4. Ensuring that all parties are aware of their responsibilities regarding IT system security incident handling, including requirements provided under the Pennsylvania Breach of Personal Information Notification Act.
5. Protecting the reputation of the College.

Definitions

1. An information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with IT operations; or significant violation of responsible use policy.

   Examples of information security incidents include but are not necessarily limited to:
   a. Computer system intrusion.
   b. Unauthorized or inappropriate disclosure of sensitive institutional data.
   c. Suspected or actual breaches, compromises, or other unauthorized access to College systems, data, applications, or accounts.
   d. Unauthorized changes to computers or software.
   e. Loss or theft of computer equipment or other data storage devices and media (e.g., laptop, USS drive, personally owned device used

for College work) used to store private or potentially sensitive information.

f. Denial of service attack or an attack that prevents or impairs the authorized use of networks, systems, or applications.
g. Interference with the intended use or inappropriate or improper usage of information technology resources.

While the above definition includes numerous types of incidents, the requirement for central security incident reporting, regardless of malicious or accidental origin, is limited to serious incidents as defined below.

Occurrences such as incidental access by employees or other trusted persons where no harm is likely to result will usually not be considered information security incidents.

2. Any serious incident is an incident that poses a threat or may pose a threat to College resources, stakeholders, and/or services. An incident is designated as serious if it meets one or more of the following criteria:
   a. Involves potential, accidental, or other unauthorized access or disclosure of sensitive institutional information (as defined below).
   b. Involves legal issues including criminal activity, or may result in litigation or regulatory investigation.
   c. May cause severe disruption to mission critical services.
   d. Incident includes active threats.
   e. Incident is widespread.
   f. Incident is likely to be of public interest.
   g. Incident is likely to cause reputational harm to the College.

3. Sensitive institutional information is defined as information whose unauthorized disclosure may have serious adverse effect on the College's reputation, resources, services, or individuals. Information protected under federal or state regulations or due to proprietary, ethical, or privacy considerations will typically be classified as sensitive. Sensitive information includes personally identifiable information such as protected health information (PHI), Federal Education Right to Privacy Act (FERPA) protected information, “personal information” as defined under the Breach of Personal Information Notification Act (PI), Social Security numbers, credit card numbers, and any other information designated as sensitive by the College.

Scope

This policy is platform and technology neutral, and applies to the entire College, including the Schnecksville Campus, Center City Allentown Campus, Allentown airport facility, Tamaqua, and any and all other College facilities.

Specifically, the scope of this policy includes and encompasses:

- Faculty, staff, and students;
- Third-party vendors, who collect, process, share or maintain College institutional data, whether managed or hosted internally or externally;
- Personally owned devices of members of the College community that access or maintain sensitive institutional data.

Guidelines

1. All users of College IT resources must immediately report all information security incidents to:
   a. The College Information Security Officer (ISO) at helpme@lccc.edu
   b. The employees’ direct supervisor
   c. Director of Human Resources

2. Any information security incident of College information must be reported.

3. It is expected that incident reporting, from identification to reporting, will occur as soon as possible and no later than within 24 hours.

4. Some information security incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and should immediately be reported to the College Office of Public Safety and Security concurrent with the incident notification described within this policy.

5. To avoid inadvertent violations of state or federal law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity before making the notifications required by this policy, except where necessary to comply with a court order or a directive of law enforcement.

6. Privacy and Confidentiality of Sensitive Information:
    a. Information related to campus security information security incidents is classified as sensitive under LCCC's Policies & Regulations Manual, Policy 3-236, Technology – Institutional Data Security.
    b. When College staff report, track, and respond to information security incidents, they must protect and keep confidential any sensitive information.
    c. Incident data retained for investigation will exclude any sensitive information that is not required for incident response, analysis, or by law, regulation, or College policy.

Roles and Responsibilities

A. The College Chief Information Officer acts as a resource for interpretation and implementation of this policy, as well as for coordinating serious information security incident communications. The College Chief Information Officer, in carrying out his/her duties, may consult with the College Information Security Officer (ISO). The Office of the College Human Resources will be provided with and retain relevant records and evidence pertaining to all serious incidents for a period of three years after the occurrence of the event. For incidents involving unauthorized disclosure of PHI, PI, or FERPA records will be retained for six years. The Chief Information Officer and Director of Human Resources will, in addition, oversee the completion of all legally necessary reporting and notification obligations.

B. College Information Technology department will oversee, coordinate, and guide the incident management process to promote a consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations.

C. All IT staff serve as the information security provider for Information and Technology Services and all College campus locations.

D. The *ISO* shall

1. Convene, when appropriate, a multi-•- department Computer Security Incident Response Team (CSIRT) including to be comprised of human resources, supervisor, and the vice president in charge of the area.

2. Collaborate and coordinate with other College offices including applicable compliance and communication offices.

3. Take appropriate steps to preserve forensic evidence.

4. Lessons learned meetings should be conducted for all serious information security incidents to review the effectiveness of the incident handling process, prevent recurrence of similar incidents, and identify potential improvements to existing security controls and practices.

5. Conduct ongoing information security incident reporting education and awareness for the College community.

E. Users of College Information Technology Resources: All faculty, staff, and workforce members must report serious information security incidents to the ISO and the College IT Service Desk within 24 hours of becoming aware of the incident.

1. All incidents must be reported to the ISO and CIO at (helpme@lccc.edu)
2. If an incident involves a potential crime it must be reported to the College Department of Public Safety immediately via email.
3. If an incident involves payment card information (PCI), the College merchant must report the incident to the Chief Financial Officer immediately via email.

F. The College FERPA Officer, Director of Registration and Student Records, will inform ISO of serious incidents reported to them.

G. Third Party Vendors and Contractors: The College has an ownership, stewardship or custodial interest in all College data, parties that are contractually bound to limit the access, use, or disclosure of College information assets. These third party vendors or entities shall report potential or actual incidents to the College per the terms of their contract and/or the College's data protection addendum.

Violations and Sanctions

Violations of this policy may result in disciplinary action up to and including suspension or revocation of computer accounts and access to networks, non-reappointment, discharge, dismissal, and/or legal action per LCCC’s Policies & Regulations Manual.

In addition to College disciplinary actions, individuals may be personally subject to criminal or civil prosecution and sanctions if they engage in unlawful behavior related to applicable federal and state laws.