Administrative Guideline 1116

ADMINISTRATIVE GUIDELINE TYPE: Information Technology
ADMINISTRATIVE GUIDELINE TITLE: Employee Guidelines for Reporting Security Incidents

DEPARTMENT RESPONSIBLE: Information Technology
GUIDELINE STATEMENT OF PURPOSE: Employee Guidelines for Reporting Security Incidents

1. Statement of purpose

Southeastern Community College recognizes the importance of protecting our employees, students and community members from unauthorized access of confidential information. In addition, the College recognizes the importance of protecting our systems (computers, servers, databases, network, etc.) from intrusions causing harmful outcomes such as denial of service and unauthorized access to private data.

The following guideline defines SCC's process to identify, communicate and resolve security incidents in an efficient manner.

The SCC ITS Office is responsible for assisting in responding to IT security related incidents. A security related incident may include unauthorized access to your computer and/or the misuse of SCC IT resources, including the unauthorized acquisition, disclosure, or modification of confidential data.

2. Definitions

Security incident definitions and examples are provided below. Please note that any suspicious activity should be reported.

A. Data Incident – any situation where an employee believes confidential data has been accessed by an unauthorized person or entity. Examples are provided below:

- Laptop Computer is stolen or misplaced that stores confidential data
- Mobile disk (USB drive, floppy, etc.) has been stolen or misplaced
- SCC Web site is publishing confidential data
- Paper documents (reports, files, etc.)
- Email asking for confidential data

B. System Incident – any situation where an employee believes a system is accessed by an unauthorized person or entity. Examples are provided below:

- Virus software communicates a virus or worm on your computer
- Changes to your system that you were not aware of such as a new screensaver, pop up messages, another person's login, etc.

3. Incident Response Process

All SCC employees should adhere to the following process when reporting a security incident:

A. Employee will complete Security Incident Form from SCC Security Website
B. Contact SCC's Chief Security Officer at 319-750-9485 and communicate the issue. Please note this number is available at all times.
C. Chief Security Officer will involve the appropriate ITS staff to identify and resolve the issue.
D. ITS will document incident details on the IT Security Incident Log
E. Chief Security Officer will contact the originator for follow up purposes
F. If critical data is compromised, Chief Security Officer will immediately contact Human Resources to determine next steps

4. Incident Reponses Management

The following incident management processes will be followed by the ITS Division:

A. ITS staff will log all incidents.
B. Chief Security Officer will present log at monthly Security Committee Meetings
C. Security Committee will identify trends and gaps that may require revisions to Security Policies and Guidelines