

College Operating Procedures (COP)



Procedure Title: Security Incidents
Procedure Number: 02-0404
Originating Department: Technology Services

Specific Authority:

Board Policy 6Hx6:2:00
Florida Statute 1001.65
Florida Administrative Code Chapter 815 – Computer Crimes Act

Procedure Actions: Adopted: 4/9/08; 02/10/09

Purpose Statement: The purpose of this document is to define the procedure for reporting possible security violations.

Guidelines:

Florida SouthWestern State College Technology Services monitors and responds to reported security violation incidents.

Procedures:

- I. If any Technology Services staff member is made aware of a possible security violation, they will immediately notify via email their supervisor and the CIO – Technology/ Research.
- II. The staff member and supervisor will work with the IT Manager – Networks and Security to conduct initial research into the possible security violation. The IT Manager – Networks and Security will add an entry into the on-going Security Issues Log and complete the Incident Report. The incident reports are kept in the Network Security folder.
- III. If it should appear that the violation has likely resulted in a violation of the Florida SouthWestern State College Appropriate Use policy, the CIO – Technology and the IT Manager – Networks and Security will immediately notify the Florida SouthWestern State College Director of Public Safety.
- IV. The CIO – Technology and the Director of Public Safety will direct their staff to complete a Security Incident form.
- V. The Director of Security will initiate a formal investigation into the possible security violation.
- VI. If the initial research (step II above) should result in clear evidence that there was no security violation, a summary of the incident circumstances will be sent via email to the

Director of Public Safety and the CIO – Technology. These emails will be retained for one year.

Network and Security Incident Report

To: *(Recipient)*

From: *(Author)*

Date: *(Date the report was written)*

Re: *(Location of the outage)*

Impact: *(Type of outage and who suffered from the event)*

Systems Affected: *(Malfunctioning system or environment that caused the outage)*

Start Time: *(Start time and date of the event)*

Final Resolution Time: *(Resolution, time and date)*

Status: *(Status of the environment at the time of the report)*

Situation:

(Record the start of the event and include the time, date symptoms, and first actions taken.)

Next Steps:

(Record the following steps taken to resolve the issue. The entry should include times, dates, and positions involved in the resolution of the event.)

Resolution:

(Record the final resolution or root cause of the event.)

How to keep this from happening again:

(Record any new information gathered from the event that will involve steps to be taken to avoid a reoccurrence of the outage.)