**Policy No: 813**
**Area: Information Technology Services**
**Adopted: 8/6/2012**

# Information Security Operational Procedures
# Procedure for Identification of a Departmental Security Contact

## PURPOSE

The purpose of this policy is to ensure that the campus departments can be contacted in the event of a computer or network security incident. The ability to quickly contact responsible departmental personnel and have them take appropriate action can mitigate negative effects of an incident both locally in the department and more globally throughout the campus and the Internet.

## BACKGROUND

Like many university campuses, Central State University (CSU) is experiencing an increase in unauthorized attempts to access its network and computer systems. Attempts to break in to campus computers are a regular event.

Risks to our academic mission are very serious. The loss or corruption of information or access to information on research or instructional workstations and servers, student records, and financial systems could greatly hinder campus work. The campus has a responsibility to secure its computers, networks and to respond quickly to threats to the integrity of systems and data. A compromised computer in one department can easily be used as a springboard to launch attacks on computers in other departments or the Internet.

Because of these risks, Division of Information Technology & Services (ITS) personnel must take action when they become aware of a security incident specifically involving a CSU resource. In cases where the incident poses a potentially serious threat to campus information system resources or the Internet, the computer will be immediately blocked from network access as detailed in the document Procedures for Blocking Network Access.

When a problem computer is identified, whether or not it is blocked from network access, campus security personnel must be able to quickly contact someone in the appropriate campus department who can take action and/or pass the information on to the appropriate departmental personnel. Quickly reaching a departmental contact is also important so that any affected user(s) may be informed of the situation. In addition, ITS security personnel will inform this contact

person of possible irregularities such as computers with configuration problems that could negatively impact the network or that appear to be infected with a virus.

## REQUIREMENTS:

To implement this procedure, each department will appoint a security contact and one or more backup contacts. Groups of departments may agree to share contacts for efficiency. Security contacts need not be technology experts, but a reasonable level of technical knowledge is helpful. Contacts may be faculty or staff as nominated by department chair, dean, or supervisor and must have an acceptable background check by Public Safety. Contacts should be available for training and consultation. They should possess effective communication skills as they will be educating their user base as necessary regarding security policies and procedures.

Security contacts must respond to security incident reports from campus security staff and pass them on to responsible departmental personnel or request Help Desk support (SERVE) as appropriate. Contacts must be knowledgeable with the computers in their departments and be able to determine who a responsible technical person is; it is not necessary for the contact to have an extensive security expertise.

Security contacts are responsible for ensuring that appropriate personnel take action in response to each security incident, including escalating the incident to an appropriate departmental authority if action is not taken and that resolution of each incident is reported to cio@csu.edu.