EMPORIA STATE UNIVERSITY™

Information Security Procedures, Standards and Guidelines			
Policy(ies) affected:	Information Security 5.1.1 Incident Response 13.1.1		
Type of document:	IS Incident Response Procedures		
Description:	Procedures for reporting information security incidents	Last updated:	January 11, 2012

Purpose of these Procedures

Information Security needs to be regarded by all Emporia State University computing users. When security incidents happen, serious threats and consequences can occur. ESU students, faculty and staff are responsible for reporting suspected or known security incidents, including any observed or suspected security weakness in ESU systems or services.

Procedures

Incident Reporting

1) An Information Security Incident can be an example of:
   a. Your computer or laptop is missing
   b. Your ESU network account is being used when you were not using it
   c. When you left for the day/week, you powered off your ESU computer. You return to work and find your computer is turned on and work files are on the screen
   d. As you power up your ESU computer and enter your password, you notice the logon field does not show your UserID, but someone else's UserID
   e. You discover that some of your files are renamed or missing
   f. You receive an unexpected call from someone who identifies themselves as an TCS support person and asks for your password
   g. You observe a stranger moving or removing desktop computers, attempting to access a restricted area without identification or wander around your work area with no apparent reason for being there
   h. You receive an email asking for your username and password to keep your email or network account active
   i. You receive an email with an attachment that you were not expecting
   j. You notice unsafe information protection practices happening
2) All suspected high severity incidents (i.e. those involving possible breaches of personal identify information) must be reported directly to the Information Security Officer (ISO) as quickly as possible by phone (preferred), email, or in person:

   Cheryl O'Dell
   004 Butcher Education Center
   Emporia, KS 66801
   PHONE: 620-341-5969
   Email: codell@emporia.edu

   If the ISO is not available, contact the Chief Information Officer (CIO):

   Michael Erickson
   003 Butcher Education Center
   Emporia, KS 66801
   PHONE: 620-341-5297
   Email: mericks2@emporia.edu

3) All other suspected incidents must be reported to any of the following:
   a. Send email to iso@emporia.edu (preferred)
   b. Contact the ISO above
   c. Contact the network security analyst at sshoemak@emporia.edu
   d. Contact the CIO above
   e. Contact the TCS HelpDesk
4) At times, an ESU community member may want to remain anonymous reporting the incident. If anonymity is necessary to report a security incident, the ISO may not be able to conduct a thorough investigation. Confidentiality is a key part of security incident investigations. If the ESU community member still feels uncomfortable reporting the incident, an external (3rd party) email account may be used to contact the ISO.
5) **Warning**: If reporting a suspected security weakness or system vulnerability, do not attempt to confirm it by testing the weakness since that could be interpreted as a potential misuse of the system or cause damage to it.
6) When receiving a report of a suspected or confirmed security incident, the ISO or designee will gather as much of the following information as possible:
   a. Name, affiliation, email address, and phone number of person reporting the incident
   b. Description of the suspected security incident
   c. Information to help identify the source of the suspicious activity, like an IP address or an email message with full headers.
   d. Date(s) and time(s) of the suspicious activity, noting the time zone.
   e. Evidence of suspicious activity (for example, full headers of an email message suspected to be spam originating at ESU, appropriate log records, etc.)
7) In addition to documenting the initial report, the ISO or designee will:
   a. Initiate appropriate incident handling procedures
   b. As appropriate, communicate with and provide feedback about the results to those reporting the incident once the incident has been handled and closed.

Incident Detection

8) In addition to reports from the university community of suspected or confirmed security incidents, anomalous events may be detected that indicate potential security incidents. Having mechanisms to detect anomalous events early and reliably helps minimize their impact. Detection can be very challenging since there are potentially so many different types of incidents and vectors for attack on a large number and variety of systems and networks. Therefore, a variety of TCS personnel and department technical liaisons work collaboratively to detect threats.
9) Channels for detecting possible security incidents include:
   a. Email sent to iso@emporia.edu
   b. Email sent directory to the ISO, CIO or network security analyst
   c. Phone call to ISO or CIO
   d. REN-ISAC, State of Kansas Security Office, or KanREN notification of suspected malicious activity

e. Network performance monitoring
f. Notification from a copyright owner or representative sent to ESU's designated copyright agent
g. Court orders
h. Customer contacting the HelpDesk
i. Monitoring security mail lists and web sites for threat alerts