



Take a second
to be secure.

The Security Minute

A communication of the Longwood University Information Security Office

Read *The Security Minute* Online: www.longwood.edu/infosec

February 2011

IN THIS ISSUE


SECURITY SPOTLIGHT:
FACEBOOK + HTTPS = YES!

TELL ME ABOUT IT...
A REVIEW OF INCIDENT
REPORTING GUIDELINES.

THANKS

We're on
 **acebook!**
LongwoodInfosec

Security Spotlight:

 + HTTPS =
YES! where,
FB=Facebook
HTTPS=Translator

Facebook has a new account setting that allows you to encrypt data in transit throughout your session. HTTPS provides additional security by protecting your private information from people who want to steal it. If you access Facebook from many locations it's recommended that you enable this new security feature. *more information is available at:*

www.facebook.com/LongwoodInfosec

Policy 6103: Encryption Policy

Policy 6132: Incident Response

Policy 6134: Data Classification

Policy 6135: Security Roles and Responsibilities

Thank You for participating in our IITS Policy Review Process on Blackboard. These policies have been submitted for approval during the Board of Visitors Meeting in March. Final drafts are available on Blackboard.

More information is available at:
www.longwood.edu/infosec/policyreview.htm

Tell Me About It...: With an updated version of the Incident Response Policy Pending BOV approval this seems as good a time as any to review the Incident Reporting Guidelines.

What's an Incident? A computer incident is any adverse event that threatens the confidentiality, integrity, or availability of university information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or a standard computer security practice is an incident. Incidents may include, but are not limited to, malware affecting multiple systems, unauthorized intrusion or damage to web site or page, unauthorized intrusion into a computer system or network or other threats.

What should I do?

- Do not panic.
- Do not make changes to the system or the device unless that system or device is under threat of attack, compromise, or loss of data.
- Report the suspected incident.
- Do not attempt to gather any information or evidence from the device, wait for the Incident Responders to arrive.

Who should be notified? As an Incident Discoverer (Fig. 1), it is your responsibility to report the suspected incident to

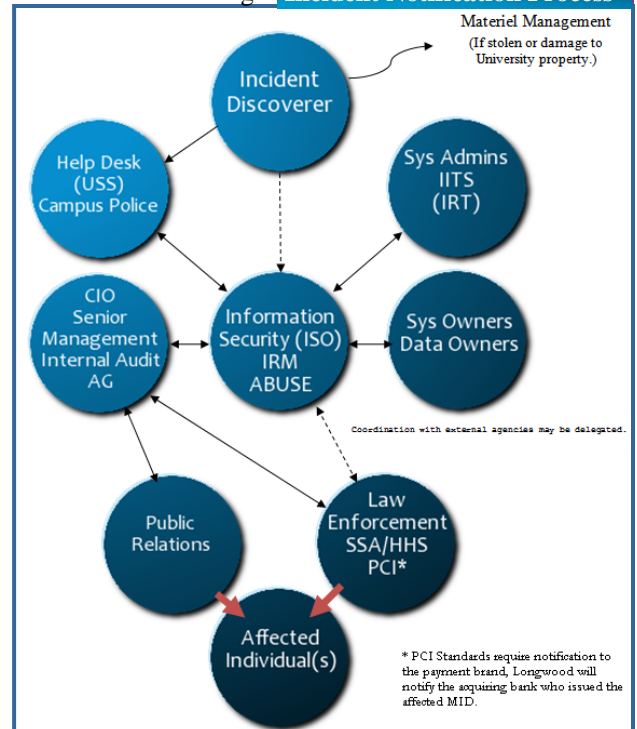
- x4357..... Helpdesk
- x2091..... Campus Police (after hours)
- x2034..... Information Security

What happens next? After reporting the suspected incident

- Await Campus Police or the IITS responder.
- Be prepared to answer questions. If you had to take measures or actions to protect the system or data be prepared to explain in detail the actions you took and why.
- You may be asked to further assist the investigation by the IITS responder.

More information is available at: www.longwood.edu/infosec/violation.htm

Fig 1. Incident Notification Process



The Security Minute is a monthly publication aimed at raising awareness of information security related issues and concerns. Please contact Jennifer Eckrote at 434-395-2034 or eckrotejl@longwood.edu.