What information should I provide?

Include a complete description of what you have observed or why you suspect an incident.

Also provide:

- Your contact information (name, phone number, e-mail address, department)
- Time and location of the incident
- If your report involves e-mail, forward the complete message including the headers and routing information
- If your report involves a web page, include the complete URL (web address) and describe the problem

Contact Information:

Helpdesk ..... 4357 (HELP)

Campus Police 2091

or

abuse@longwood.edu

More information regarding Incident Response is available:

University Policy 6132
INCIDENT RESPONSE

http://www.longwood.edu/infosec/policies.htm

Info Sec

LONGWOOD UNIVERSITY

201 High Street
Farmville, VA 23901
infosec@longwood.edu

Phone: 434-395-2034
Fax: 434-395-2035

Computer Incident Response

What should I do?

This document serves as a general guideline for individuals discovering or alerted to potential incidents that involve IT resources and systems.

LONGWOOD
UNIVERSITY

INFORMATION SECURITY

February 2011

Incident Response: What should I do?

What are computer incidents?

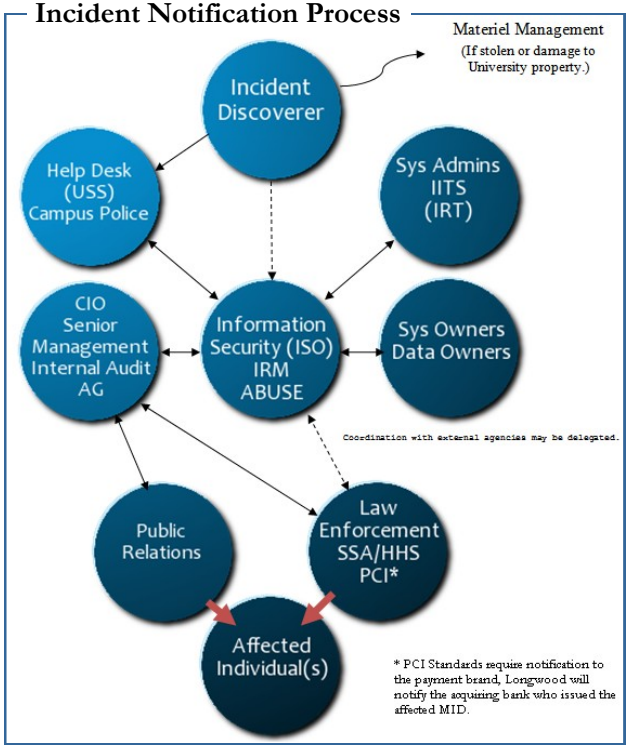
A computer incident is any adverse event that threatens the confidentiality, integrity, or availability of university information assets, information systems, and the networks that deliver the information.

Any violation of computer security policies, acceptable use polices, 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.

Threats, harassments, annoyances, and intimidation of any kind over electronic media should be reported to Campus Police immediately.

Incident Notification Process



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.

What should I report?

Examples of incidents that should be reported include:

- Unauthorized access to a computer or account.
- Damage or vandalism to IT equipment.
- Theft of IT equipment.
- Malware (viruses, worms, Trojans, or other malicious software.
- Compromises of University data.
- Violations of University IT policy.

Who should be notified?

As an Incident Discover, it is your responsibility to report the suspected incident to

- the Helpdesk
- Campus Police (after hours)
- Information Security