

Best Security Practice for
REPORTING ELECTRONIC SECURITY INCIDENTS

PUBLISHED BY THE OFFICE OF INFORMATION TECHNOLOGY – MARCH 2008
"BEST PRACTICES ARE THE PROCESSES AND ACTIVITIES THAT HAVE BEEN SHOWN TO BE THE MOST EFFECTIVE"

BEST SECURITY PRACTICE (BSP) No. 5: *IT IS THE RESPONSIBILITY OF ALL UNLV IT SYSTEMS USERS, OWNERS AND MANAGERS TO REPORT ALL UNACCEPTABLE USE AND ALL BREACHES OF INFORMATION SECURITY OR SECURITY INCIDENTS, ACTUAL OR SUSPECTED, PROMPTLY TO CAMPUS COMPUTING SERVICES(CCS), OR TO THE LOCAL SYSTEM SECURITY LIAISON, OR TO THE UNLV INFORMATION SECURITY OFFICE (ISO). [THE TERM "SECURITY INCIDENT" IS DEFINED AS ANY IRREGULAR OR ADVERSE OR MALICIOUS EVENT OR USE THAT THREATENS THE SECURITY, INTEGRITY, OR AVAILABILITY OF THE INFORMATION RESOURCES OR PERSONNEL ON ANY PART OF UNLV'S NETWORK.]*

OBJECTIVES: To provide direction and support for information security in accordance with internationally accepted standards (ISO 17799/27001), business requirements and relevant State and Federal laws and regulations. This technical Best Practice directly supports the UNLV Capstone Policy IS01 - Information Security for Information Resources and Asset, and defines the acceptable use of UNLV information technology services and accounts. **This Best Practice is also mandated under UNLV Reporting Electronic Security Incidents Policy (IST104).**

BACKGROUND: Dependencies on technology to support business functions and delivery of UNLV programs expose the operational environment to risks of accidental and intentional security breaches. Reporting of suspected security incident occurrences improves the overall security posture of UNLV by initiating a systematic process of security incident management..

The last part of this BSP, "**General Violations of Acceptable Use of IT Systems,**" contains a reminder list of possible general violations that may constitute an incident – it is not exhaustive.

The purpose of this Practice is to:

- Ensure that access to UNLV electronic resources remain secure according to their risk factors.
- Establish the mandatory reporting of suspected information security incidents.
- Establish adjunctive policies on incident response and communications;

In order to manage information security comprehensively, this Best Practice serves the to:

- Ensure that use of IT systems is consistent with sound security principles;
- Ensure that IT systems are used for their intended purposes and meet any compliance requirements;
- Ensure the confidentiality, integrity, availability, and superior performance of IT systems;
- Assure that the core IT network and systems is available to support emergency services in the event of community disaster response needs; and
- Establish standards for addressing security consistency.

AUDIT CONTROL: Security audits will inspect the in-use organization security incident reporting procedures, and processes by using this best practice as the compliance base. This Best Practice will be audited using the appropriate BS 7799.2:200x Audit Check List, dated 8.08.2005 or later, and through a complete review of all related complaints (security incidents) that occurred after the previous audit.

BEST SECURITY PRACTICE STANDARDS

INFORMATION SECURITY STANDARDS AND CONTROLS. The following are the Best Practice Standards that should be applied to be in minimum compliance with UNLV standards.

BSP: 5-1 User and System Provider Reporting of Incidents. Management, all users, and systems personnel should report all unacceptable use and electronic security incidents promptly and to the appropriate office or group. If you believe that a violation of this policy has occurred, contact the system or network administrator responsible for the system or network with the problem. That person will report the incident to the appropriate information security personnel in accordance with reporting guidelines.

BSP: 5-2 User and System Provider Response to Incidents. Management, all users, and systems personnel should follow the appropriate steps defined under the guidelines below.

SECURITY INCIDENT REPORTING GUIDELINES

Proper detection and response to incidents that may impact the integrity, confidentiality or availability of these resources is critical to the University and any individuals involved. Such incidents include, but are not limited to: virus outbreaks, physical or remote security breaches, denial-of-service attacks, and other exploited vulnerabilities.

**** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ** NOTE ****
Special care needs to be taken to ensure that personal safety is not jeopardized by an incident or by the response/non-response to an incident. Examples of incidents that could endanger personal safety might include stalking, threats of physical harm, loss of access to patient data, or failure of environmental systems.

INCIDENT DEFINITION

A security incident is defined as a compromised or suspected compromised system; any type of attack levied on or from an UNLV computer resource; or misuse of IT resources (such as chain letters, virus hoaxes, etc.). Unacceptable use incidents should be treated and processed as a security incident.

INCIDENT DETECTION

Computer users and administrators should be alert for symptoms that indicate an intrusion into or misuse of their systems. The following points are helpful in detecting intrusions:

Be suspicious of unusual activity - Unusual computer or network activity can be an indicator of a malware, attack, or intrusion. Activities and symptoms to look for include:

- Excessive malware warnings or personal firewall pop-up messages
- Unexpected system reboots and/or sudden degradation of system performance
- Unauthorized new user accounts or altered passwords
- New directories or files, often with unusual names such as "... " or " .."
- Modification or defacement of web sites.
- New open network ports on a system.
- Unexpectedly full disk drives.

Listen to complaints received from others - Comments or emails claiming suspicious activity from a computer may indicate the computer is infected or has been compromised and may actively be attacking other computers.

Other symptoms that may indicate an electronic security incident include, but are not limited to: unusually sluggish computer performance or network access, applications and/or windows opening without user prompt; generation of spontaneous emails; strange characters appearing in documents; system rebooting or shutting down for no apparent reason.

Computer administrators should be aware of the physical environment - Access to secure computing areas, such as, server rooms, telecom closets and research labs, should be restricted. Situations to be aware of include:

- Unauthorized personnel in secure areas
- Unknown users at a computer
- Missing or moved equipment

- Open or unlocked doors

Computer administrators should review logs - Logs files are invaluable in detecting and tracking attempted intrusions and other suspicious activity. To maximize the value of logs:

- Ensure that a high level of logging is enabled.
- Check logs regularly for suspicious activity and entries
- Look for missing time spans in logs
- Check for repeated login failures or account lockouts
- Investigate unexpected system reboots

STEPS

USER STEPS

If you suspect that an electronic security incident may have occurred or may be imminent, you are expected to take the actions detailed below.

1. Contact the local system or email support provider, as appropriate, of the specific computer service or IT device. Provide any necessary or requested follow-up information.
2. In the event that the local system provider or the Campus Computing Services help desk is unavailable, disconnect the affected computer or IT device from the network by disconnecting the Ethernet plug in the back of the machine and notify UNLV Campus Computing Services help desk or NOC personnel as soon as possible.

◆ Note: In circumstances where the user is also the local support provider, the user is obligated to follow the procedures listed under "Local System Provider," below.

LOCAL SYSTEM PROVIDER STEPS

When you have notified the local system provider of a electronic security incident, the provider will respond with a series of steps outlined in the internal OIT Incident Response Procedures. These will probably include:

1. Disconnecting the computer or IT device from the network or take other actions that will otherwise limit damage to other IT resources.
2. Collect all of the following relevant information.
 - a. Date and time of the incident, indicating time zone.
 - b. IP and MAC address of the affected computer or IT device, if known
 - c. Other relevant IP and MAC addresses, if known (e.g., other IT devices affected, attacking source, etc.)
 - d. Function of affected computer or IT device (e.g., desktop computer, printer, scanner, production server, development server, file server, web server, workstation, lab device, etc.)
 - e. Distinguishing characteristics of the IT device (e.g., operating system, applications installed on the information technology device, presence of anti-virus software, firewalls, other security software, etc.)
 - f. Description of the incident, including any relevant log entries, error messages, or other evidence indicating a problem with the IT device in question.
3. Notify IT security personnel via Campus Computing Services (CCS) Help desk or at the Network Operations Center (NOC).
4. Upon performing remedial actions, notify Campus Computing Services or the NOC for accurate closure of the problem report.
5. Notify affected user of remedial steps taken, recommended mitigating activities and other appropriate information.

General Violations of Acceptable Use of IT Systems.

Under no circumstances is anyone authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing UNLV-owned resources. The following activities are, in general, representative of violations.

◆ Note: Selective UNLV personnel may be exempt from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

The list is not intended to be exhaustive, but attempts to provide a framework of activities which fall into the category of unacceptable use.

- a. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by UNLV or the individual.
- b. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which UNLV or the User does not have an active license is strictly prohibited.
- c. Using a UNLV computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace policies or laws.
- d. Using UNLV IT resources for harassing, cyberharassing, stalking, cyberstalking, or threatening use is strictly prohibited. This category includes, for example, display of offensive, sexual material in the workplace and repeated unwelcome contacts with another.
- e. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- f. Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained.
- g. Circumventing user authentication or security of any host, network or account.
- h. Unauthorized access to data or files even if they are not securely protected (e.g., breaking into a system by taking advantage of security holes, or defacing someone else's web page).
- i. Intercepting digital telephonic or network transmissions, including wireless transmissions (e.g., running network sniffers without authorization).
- j. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of assigned responsibilities. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- k. Scanning of computer ports or security settings is expressly prohibited unless appropriate information technology authority's authorization is obtained.
- l. Introducing malicious programs or malware into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- m. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- n. Interfering with or denying service to any user other than the user's host (for example, denial of service attack).
- o. Making fraudulent offers or fraudulent purchases of products, items, or services originating from any UNLV network or system account.
- p. Providing information about, or lists of, UNLV employees to parties outside UNLV unless authorized to do so.
- q. Exporting software, technical information, encryption software or technology, in violation of international or U.S. export control laws. Such activity is illegal.
- r. Using IT systems in a way that suggests University endorsement of any political candidate or ballot initiative is also prohibited. Users must refrain from using IT systems for the purpose of lobbying that connotes University involvement, except for authorized lobbying through or in consultation appropriate legal counsel.
- s. Using IT systems in a way that may cause harm to other IT systems or to the integrity of any State of Nevada institution.
- t. Sending or forwarding non-UNLV (e.g., non-University related) unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam). Normal University person-to-person, department-to-person, or UNLV-to-person email communications are exempt.

- u. Any form of harassment, cyberharassing, stalking, cyberstalking, or threats via messaging or email, whether through image, language, frequency, or size of messages.
- v. Unauthorized use, or forging, of email header information.
- w. Soliciting or subscribing of email using another person's email address with the intent to harass or to collect replies.
- x. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- y. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (i.e., newsgroup spam).
- z. Complete coverage of email and IT communications policies are contained in the UNLV Email Usage Policy and the UNLV Access to Email Accounts Policy.