

*Best Security Practice for*  
**WHAT TO DO FOR A COMPUTER SECURITY INCIDENT**  
(FOR SYSTEM AND SECURITY ADMINISTRATORS)

*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. 6:** *IT IS THE POLICY AND PRACTICE OF UNLV TO RESPOND TO ALL REPORTED UNACCEPTABLE USE AND BREACHES OF INFORMATION SECURITY OR OTHER SECURITY INCIDENTS, ACTUAL OR SUSPECTED. ALL SUCH EVENTS SHOULD FIRST BE RESPONDED TO BY THE SYSTEM PROVIDER (THE "FIRST RESPONDER") AND THEN, IF WARRANTED, INVESTIGATED BY THE UNLV INFORMATION SECURITY OFFICER OR DESIGNEE.*

**\*\* 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.*

*[THE TERM "SECURITY INCIDENT" IS DEFINED AS ANY IRREGULAR OR ADVERSE OR MALICIOUS EVENT OR USE THAT VIOLATES ANY STATE, FEDERAL, OR NSHE STATUTE, ACT, CODE, OR LAW, OR THREATENS THE SECURITY, INTEGRITY, OR AVAILABILITY OF THE INFORMATION RESOURCES OR PERSONNEL ON ANY PART OF UNLV'S NETWORK. THIS COULD BE A CONFIRMED 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.).]*

---

**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. Prompt and consistent responses to reported unacceptable use and electronic security incidents protects and preserves the University's resources and aids in the University's compliance with applicable State and Federal Laws. **This BSP is the foundation for the forthcoming UNLV Computer Security Incident Response For First Responders Policy (IST408).**

**BACKGROUND:** UNLV's information security program initiative is to prevent, if possible, and minimize computer systems and/or data compromises. Preparation and coordination to handle a security incident occurrence improves the overall security posture of the University by providing a systematic process of security incident management.

*The remaining portion of this BSP is limited in distribution and is only available via internal UNLV mail by contacting the UNLV Information Security Office for further information and prerequisite requirements.*