

*Best Security Practice for*

## IT RESOURCES REQUIRING COMPLIANCE PROTECTION FOR SENSITIVE, CRITICAL OR REGULATORY DEFINED INFORMATION

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. 9:** *To comply with Nevada Revised Statutes and NSHE Regent's Policy on protecting digital non-public personal and other sensitive or critical information; all such classified university networks, servers and computers should employ and maintain such security devices, applications, and procedures necessary to conform to all federal, state or university mandated compliance codes, laws, regulations, and policies for protection of critical, privacy, or sensitive data (defined in the Nevada Revised Statutes and NSHE Regents Bylaws) in transit or at rest on these devices. The information technologies covered by the BSP include all data, systems, networks, and facilities administered by individual schools, departments, university laboratories, and other university-based entities that must meet the compliance standards to ensure effective prevention and detection of misuse, unauthorized access, unauthorized modification, or loss.*

---

**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 security of UNLV information technology services and accounts that must meet regulatory compliance. **This BSP is the foundation for the forthcoming UNLV Regulatory IT Compliance Policy (IST302) and UNLV Technical Security of IT Resources Policy (IST501)**

This BSP has a primary focus to standardize IT compliance regarding sensitive or critical University data and non-public privacy data of individuals; to protect the university against seriously damaging or legal consequences; to prevent the disregard of regulatory restrictions, or contractual obligations; to safeguard the integrity of computers, networks, and data, at UNLV or elsewhere; and to ensure that use of electronic information resources complies with the provisions of the Nevada System of Higher Education (NSHE) Code and University Policy.

**Compliance With NSHE Board of Regents Data Security Policy:** It is the policy of the Board of Regents, Bylaws Title 4 Chapter 1 Section 27 titled Data Security Policy, that "sensitive data maintained or transmitted by an NSHE institution must be secure. For the purposes of that Section (27), "sensitive data" means any data associated with an individual, including but not limited to social security number, employee identification number, and data that is protected by state or federal law." [See Nevada Senate Bill 347, enacted into law 6.17.2005, for amending the Nevada Revised Statutes Chapter 205, 205.461, 205.4617, 205.463, 205.464, 205.465, 205.4653, and 205.4657, Chapters 52, 597, and 97A, 97A.140, and 97A.293. See also Federal statutes.] *Extracted: "Each NSHE institution must develop and maintain policies, standards, and/or procedures that describe and require appropriate steps to protect sensitive data that is maintained on an institution's computing devices or transmitted across a public network such as the Internet. Institutional policies must include the requirements for the eradication of data when computers are sent to surplus or repurposed. Institutions must be aware of all areas that data are stored, both physically and electronically, and must audit these areas annually to ensure that sensitive data are retained or destroyed as appropriate. Each institution must maintain policies and procedures to be followed in the event that sensitive data is released inappropriately."*

***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.***