OIT Security Standards and Procedures for the Technical System Administration Policy

Introduction

In accordance with the Technical System Administration Policy, systems must meet security standards and adhere to the associated procedures set by the Office of Information Technology (OIT).

The standards below are meant to serve as a guide for technical administrators to determine appropriate security guidelines and benchmarks for university systems. Technical administrators should apply all the recommendations applicable to the systems for which they are responsible in conjunction with best practices of vendors and other security standards organizations. The procedures outlined below are designed to ensure the campus is in compliance with the Technical System Administration Policy and that the associated security standards are met. The end goal is secure systems that meet the functional and business needs of each campus unit.

Because addressing security once deployment and implementation have occurred is more difficult, security should be considered from the initial planning stage for any new system implementation.

Standards

1. Password Standards

1.1 <u>Privileged Account Password Standards</u>

1.1.1 Password Complexity

Passwords for privileged accounts must meet the following criteria:

- Be at least 12 characters
- Contain a mix of three out of the four possible character types:
  - UPPERCASE letters (A–Z)
  - Lowercase letters (a–z)
  - Numbers (0–9)
  - Symbols (! @ $ % &)
- Not use common symbol substitutions for letters (“@” for “a”; “$” for “s”)

Examples of strong, secure passwords that meet the complexity criteria include:
#45rKKvhJj9r
a56v)^iPy4KCJ

1.1.2 Reuse of Passwords

Reuse of the two most recent passwords in succession is prohibited.

Privileged account passwords should not be used on multiple accounts (e.g., domain administration password should not be used for Web server root password).

1.1.3 Password Expiration

Privileged passwords must be changed every six months.

1.2 Service Account Password Standards

1.2.1 Password Complexity

Passwords for service accounts must meet the following criteria:

- Be at least 16 characters
- Contain a mix of three out of the four possible character types:
  - UPPERCASE letters (A𝕄Z)
  - Lowercase letters (a𝕄z)
  - Numbers (0𝕄9)
  - Symbols (! @ $ % &)
- Not use common symbol substitutions for letters ("@" for "a"; "$" for "s")

Examples of strong, secure passwords that meet the complexity criteria include:

#45rKKvhJj9r*3rb
a56v)^iPy4KCJ𝕄9x

1.2.2 Reuse of Passwords

Reuse of the two most recent passwords in succession is prohibited.

Service account passwords should not be used on multiple accounts (e.g., service account password to connect Footprints to LDAP should not be used as the database synching account password).

1.2.3 Password Expiration

Service passwords are not required to expire automatically.

1.3 Exceptions to Password Standards

Any system that will support the requirements in sections 1.1 and 1.2 must be configured to do so. The technical administrator is responsible for educating users of the system on required password standards even if they cannot be mandated by the system.

If a system does not support the above requirements, the technical administrator must configure passwords of the maximum length and complexity that the system will support.

Any deviations from the requirements listed in sections 1.1 and 1.2 will require a written exception detailing the compensating security controls in place on the system. All exceptions will be audited periodically to ensure compliance with policy.

To request an exception, please complete the OIT Exception Form found at https://oit.unlv.edu/node/6022

2. Account Management Standards

2.1 Provisioning and Deprovisioning Accounts

When establishing account provisioning and deprovisioning procedures on the systems for which they are responsible, system owners shall:

- Ensure a unique account is provided for each individual authorized to access the systems for which they are responsible.
- Promptly deactivate accounts for separated individuals from any computing system at the end of the individual's employment or when continued access is no longer required.
- Remove/disable accounts of transferred individuals to ensure changes in access privileges are appropriate to the change in job function or location.
- Ensure all guest accounts with access to UNLV computing resources have an expiration date of one year or the work completion date, whichever occurs first.
- Review all accounts at least annually to ensure access and account privileges are commensurate with job function, need-to-know, and employment status. OIT may also conduct periodic reviews of accounts for any system connected to the UNLV network.

2.2 Account Privileges

When establishing accounts, the standard security principle of “least privileged access” to perform a function must be used whenever administratively feasible. For example, a root or administrative privileged account must not be used when a non-privileged account would be sufficient.

2.3 Establishing Accounts

The identity of users must be verified before providing them with account and password details. If an automated process is used, the account holder should be asked to provide several pieces of identity information that, in totality, could only be known by the account holder. In addition, the following criteria must be followed when establishing accounts:

- Passwords for new accounts should NOT be emailed to remote users UNLESS the email is encrypted.
- Stricter levels of verification (e.g., faceMtoMface) must be used for those accounts with privileged access (e.g., accounts that can be used to modify department budgets require a more thorough verification process than accounts used for email).
- Use of shared accounts is not permitted. However, a provision to support the functionality of a process, system, device (e.g., servers, switchers or routers) or application (e.g., management of file shares) may be made. In such situations, an exception including documentation justifying the need for a shared account must be requested from OIT. The documentation should include a list of individuals who have access to the shared account.

3. Security Standards

Security standards are constantly evolving. Consequently, technical administrators are expected to follow current industry security best practices appropriate for the systems within the scope of their responsibilities.

Links to the best practices for physical security, server and network device configuration, database security, and web server configurations are provided below. Additional security procedures may be necessary based on vendor recommendations and/or to meet regulatory requirements.

Systems that are unable to meet best practice guidelines will require a security exception and compensating controls.

UNLV will use the best practice resources provided below as a guide in conducting security assessments and audits.

3.1 Physical Security and Access Control

Physical networking infrastructure, servers, and other systems must be kept in a secure location where access is controlled and logged.

Locations containing these systems must be kept securely locked at all times and cannot be accessed without authorization of the system owner or accompanied by an authorized facility escort.

These locations include:

- Data center facilities
- Network and cable termination facilities

- Any similar areas containing cabling and devices for communications or networking

Access to the locations containing systems must be logged. For facilities using electronic entry systems for access for those who work in the area, the logs associated with the electronic system will suffice. A visitor log for those without electronic access cards should be kept. The logs should be audited periodically and be made available for incident investigations as well as internal and external audits as needed.

3.2 Server Security and Hardening

System hardening is the process of securely configuring computer systems to eliminate as many security risks as possible. While default security configurations for many products have improved greatly over the years, some options and settings favor ease of use over security, exposing vulnerabilities that can be used to compromise a system. Also, default configurations may not offer enough protection for systems handling sensitive information on the campus network. The resources below offer guidance on secure configurations and hardening procedures.

3.2.1 General Server Security Guidelines M specifically sections 4 through 6

http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

3.2.2 Server Product Specific Guidelines (e.g., Windows, Linux)

https://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

3.3 Network Security

All data flows through network routers, switches and firewalls. Network devices present attack points where data flows can be intercepted or disrupted. The best practice procedures described below are designed to help prevent unauthorized access to network devices.

3.3.1 Routers and Switches

https://www.nsa.gov/ia/_files/routers/c4-040r-02.pdf

The *Router Security Configuration Guide,* created in 2005, remains the most frequently cited vendor neutral reference for securing routers.

3.3.2 Firewalls

http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

3.4 Database Security

Databases often store sensitive and business critical data for an organization. Hackers increasingly target databases to obtain sensitive personal and financial information. Protecting databases and the underlying systems that support them against the risk of breach and data loss is vital. The best practice procedures described below are intended to help prevent unauthorized access to databases.

3.4.1 Database Security Guidelines

http://www.isaca.org/Journal/Past▯Issues/2008/Volume▯5/Pages/Database▯Security▯Compliance▯and▯Audit1.aspx

3.4.2 Database Product Specific Guidelines (e.g., Oracle, SQL)

Oracle:

http://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm M DBSEG009

SQL:

http://msdn.microsoft.com/en▯us/library/bb669074(v=vs.110).aspx

Microsoft Access:

The use of Microsoft Access databases is not recommended, as the ability to secure these databases is limited compared to other products available. System owners should strive to migrate the database to a more secure product. If Microsoft Access must be used for compatibility reasons, the security guidelines below should be followed.

The guidelines are from the collection of Department of Defense Security Technical Implementation Guides (STIGs). The link below lists all of the available STIGs. You should use the one applicable to the version of Microsoft Access you are using.

http://iase.disa.mil/stigs/Pages/a▯z.aspx

3.5 Web Servers

Web servers are often the most targeted and attacked hosts on an organization's network. Web servers may also face indirect attacks to gain information from its users. Consequently, it is essential to secure web servers and the network infrastructure that supports them.

http://csrc.nist.gov/publications/nistpubs/800-44-ver2/SP800-44v2.pdf

The *Guidelines on Securing Public Web Servers*, revised in 2007, remains the most frequently cited vendor neutral reference for securing web servers.

3.6 Exceptions to Security Standards

Currently, there are no predefined exceptions to the Technical System Administration Policy. Exceptions will be made on a case-by-case basis.

To request an exception, please complete the OIT Policy Exception Form found at https://oit.unlv.edu/node/6022

A written explanation as to why the system or service requires an exception must be submitted (e.g., security patch cannot be applied in an automated fashion due to the applications on the server). Technical documents should be included where available.

To protect sensitive data and preserve the integrity of UNLV systems, OIT staff will work with the requester to:

- Establish compensating controls for system operation to mitigate risk.
- Develop an audit schedule to verify the compensating controls remain in place and are mitigating current risks.

Deliberation on exception requests will begin within 10 business days of receipt of the request. Exceptions will be reviewed annually. Periodic audits will be conducted to determine that the conditions for granting the exception are still being met.

Procedures

1. Inventory of UNLV Systems

A current inventory of information technology assets allows the university to identify potential risk and establish controls to protect those assets.

System owners must report any system that contains sensitive, personal information. Reports will be made to the Office of Information Technology via the Inventory of Information Systems. More information is available at: **Under construction**

2. Audits

Auditing information systems ensures that the security standards outlined in this document and the Technical System Administration Policy are met.

Technical administrators are expected to assist with both internal (e.g., OIT, Campus Audit Department) and external (e.g., NSHE, PCIMDSS, HIPAA) audits.

Internal audits will be conducted periodically as resources allow. Every effort will be made to notify technical administrators in advance of the audits. These audits will follow the procedures outlined in the OIT Audit Framework. More information is available at: **Under construction**

External audits will follow the procedures of the entity performing the audit. For more information about external procedures, technical administrators should refer to that entity's website or contact them directly.

Definitions

Authorized facility escort – An individual who is authorized to provide access and accompany guests into secure spaces containing systems.

Guest – NonMuniversity employees who need access to university systems to assist with university business. Guests requesting university accounts must be sponsored by a fullMtime university employee. Account requests must be approved by the system owner.

Privileged account H An account used by a technical administrator with elevated access rights to one or more systems.

- Privileged accounts must be separate from a technical administrator's individual user account.
- Privileged accounts may not be used to conduct an individual's dayMtoMday activities such as accessing the Internet, email or logging into workstation.
- Privileged accounts should never be used as service accounts.

Service account M An account used by a system with elevated access rights for purposes related to the operation of a specific system.

- Service accounts should only be used by a system.
- Service accounts should never be used as privileged accounts.
- Service accounts should not be used by multiple unrelated systems.

Sensitive, personal information M Any information about the individual maintained by the university, including the following: (a) Education, financial transactions, medical history, and criminal or employment history; and, (b) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. [38 USCS § 5727(19)]

Sensitive, personal information does not include publicly available directory information that may be lawfully disclosed.

System M Related hardware components, software programs, or both that store, process or transmit data. Systems include but are not limited to network devices, appliances, physical and virtual environments, desktop devices being used as servers, and applications. Systems hosted by third party vendors are subject to this definition.

System owner M A fullMtime UNLV employee who is responsible for the system, knows the function(s) of the system, authorizes access, knows who the data owners are, and understands what data the system stores, processes, or transmits.

Technical administrators M Individuals who manage the system as the system owner or on behalf of the system owner. Technical administrators have administrative privileges (e.g., adds users, updates operating systems, defines roles, configures the application) and may be responsible for system, application, or user security. Technical administrators may also be known as Application Administrators, System Administrators, Network Administrators, Database Administrators, etc.

Frequently Asked Question for Policy Page

Do the policy and associated standards and procedures apply to servers administered by a third party?

Yes, servers administered by a third party on behalf of UNLV or any unit of UNLV (infrastructure as a service) must meet these standards. For each system administered by a third party, a full-time UNLV employee must be named as the system owner. The company providing technical administration must sign appropriate agreements to:

- Protect UNLV data
- Abide by all federal, state, and local laws and regulations that apply to UNLV (e.g., FERPA, HIPAA, PCI-DSS, GLB Act)
- Comply with UNLV internal policies.

The UNLV system owner is responsible for ensuring the third party providing technical administration is compliant with the requirements above.

In the case of software as a service (SaaS), such as Google Apps, Office365, or Workday, contractual arrangements negotiated on behalf of UNLV or NSHE will supersede this document. However, a system owner must be named to monitor compliance with and changes to contractual agreements and serve as the contact for any security issues that may arise.

Services operated on UNLV's behalf by System Computing Services require a UNLV system owner (generally an OIT staff member). The system owner must monitor compliance with service agreements and governance structures.

What is the timeline for bringing the systems I manage into compliance?

The systems should be brought into compliance as soon as possible. If you cannot bring all the systems for which you are responsible into compliance by December 31, 2015, please contact OIT for assistance.

Due to limits of the system, I do not believe I can meet some of the requirements (e.g., rotating passwords every six months). What should I do?

Contact OIT to discuss possible exceptions and compensating controls. The OIT Policy Exception Form can be found at https://oit.unlv.edu/node/6022.

I am not certain if a given account should be considered a service account or an administrative account. How do I make this determination?

Generally, if the account is being used by a system it is a service account. Accounts being used by a person are administrative accounts. If the account type is not readily apparent, please contact OIT for assistance.

I have test/development system. Does it fall under this policy?

If the test/development system processes, stores, or transmits actual university data (non𝕄fictitious), the policy applies.