SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
SECURE WINDOWS SERVER CONFIGURATION

Purpose –

The purpose of this standard is to offer guidance for the secure configuration of Windows servers attached to the computer networks owned and operated by Salt Lake County. This standard is based on industry best practices.

Employees of Salt Lake County shall follow the *Secure Windows Server Configuration Standard* as established by the Information Technology Division. The Information Technology Division will monitor and enforce compliance with this standard.

Reference –

The standards set forth herein are provided in accordance with Countywide Policy 1400, which directs Salt Lake County Information Technology to provide information technology standards. Also referencing the following:

All Countywide Information Technology Security Policies in the 1400 series

1.0 Scope

All Salt Lake County employees shall adhere to this Secure Windows Server Configuration Standard whenever they access County information technology resources and systems, any device that connects to any Salt Lake County network, or any device that resides at a Salt Lake County facility.

2.0 Definitions

Information Technology Resource(s) and/or System(s)
Computers, hardware, software, data, storage media, electronic communications (including, but not limited to, email, fax, phones, phone systems, and voice mail), networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the County's shared computing and network infrastructure.

Windows Server
A Windows server is any device that runs a Microsoft Windows operating system and provides services such as file sharing, printing, application hosting, management, or other computer services for Salt Lake County.

3.0 Standard Guidance

All County users shall follow the County's Secure Windows Server Configuration Standard, as defined in Appendix A of this document.

4.0 Exceptions

Any exceptions to this standard must be explicitly approved in writing by the Salt Lake County Chief Information Officer or their designee.

5.0 Enforcement

Anyone found to have knowingly violated this standard may be subject to disciplinary action by County disciplinary policies.

Revision History
AUGUST 2021 - MLE

Appendix A
Secure Windows Server Configuration Standard

Hardware Requirements

- Before purchase, all server hardware purchases must be reviewed and approved by the IT Division.

Operating System Requirements

- Windows operating system versions used on the County network must have Microsoft "Supported" status.
- Windows operating system versions no longer supported by Microsoft shall have additional security restrictions in place.
- Change all default passwords before deploying any new operating system.

Hardware and Software Inventory

- An accurate inventory of all Windows servers shall be maintained.
- An accurate inventory of all software installed on Windows servers shall be maintained.

Hardware Disposal

- Server hardware and peripherals no longer in service will be accepted with a completed PM2 form by the Information Technology Division for disposal through approved e-waste recycling programs.

Provisioning Requirements

- Installation sources for operating systems and applications shall be stored on securely configured systems and validated with integrity monitoring tools to ensure integrity.
- System configuration management tools shall automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals or through AD group policy.

Security Configuration Settings

- Windows servers shall be County domain members.
- Windows servers that are not County domain members may not be connected to the network unless the AD of Information Security has signed an exception.
- Windows servers shall be moved to the correct OU immediately after they are joined to the County domain.
- Windows servers shall be configured with the baseline security policy through GPO.
- System configuration management tools shall be deployed to automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
- Windows servers shall be configured with an automatic screensaver lock after a standard period of inactivity.
- Documented security configuration standards shall be maintained for all authorized operating systems and software.
- Anti-exploitation features such as Data Execution Prevention or Address Space Layout Randomization available in an operating system shall be enabled, or appropriate toolkits configured to protect broader applications and executables shall be deployed.

Endpoint Management Settings

- Windows servers will be managed by a County-approved endpoint management system (Tanium) to ensure that the operating system and third-party applications are kept up-to-date.
- Windows servers shall undergo vulnerability scans using a privileged account, which is not to be used for any other administrative activities and tied to a specific machine at specific IP addresses.

Anti-malware Requirements

- Windows servers shall run the approved County anti-malware protection.
- Centrally managed anti-malware software shall be used to monitor and defend the organization's Windows servers continuously.
- The organization's anti-malware software shall be regularly configured to update its scanning engine and signature database.
- Windows servers shall be configured to conduct an anti-malware scan of files on removable media automatically.
- Windows servers shall be configured by default, not to auto-run content from removable media.
- Windows servers shall be configured to send all malware detection events to enterprise anti-malware administration tools for analysis and alerting.

Application Requirements

- Windows servers must have a valid license for all installed applications.
- Only software in the authorized software inventory, as defined by the County agencies, will be installed or used on Windows servers.
- Unauthorized software shall be removed, and the inventory will be updated accordingly.
- Software deemed to be a security risk will be removed, and the inventory will be updated accordingly.
- Windows servers shall be physically or logically segregated from other systems on the County network based on the purpose of the server and installed applications.
- Change all default passwords before deploying any application.

Browser and Email Requirements

- Windows servers shall not be used to connect directly to the Internet or browse the Internet unless a signed exception has been completed.
- Only fully supported web browsers will be allowed if Internet access is permitted by signed exception.
- Windows servers shall not be used to access email services unless a signed exception has been completed.
- Only fully supported email applications will be allowed if the signed exception permits email access.
- Windows servers should not have any MS Office applications installed unless a signed exception has been completed.

Account Configuration and Use

- Accounts used on Windows servers shall comply with County IT standards for Privileged Access Management.
- Regular user accounts will not have administrative rights on Windows servers.

Logging and Monitoring Requirements

- Windows servers must be configured to use at least three synchronized time sources to retrieve time information regularly so that timestamps in logs are consistent.
- Windows servers must have local logging enabled and configured to IT Division specifications:
  - Event source
  - Event date
  - Current user
  - Event timestamp
  - Event source addresses
  - Event destination addresses and
  - Other as specified by GPO.
- Enable Domain Name System query logging to detect hostname lookups for known malicious domains.

- Enable command-line audit logging for command shells, such as Microsoft PowerShell and Bash.
- Ensure that all Windows servers that store logs have adequate storage space for the logs generated until they can be transferred to a central log management system.
- Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.
- Logs shall be reviewed regularly to identify anomalies or abnormal events.
- Monitoring systems will alert when users deviate from normal login behavior, such as time of day, server location, and duration.