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

Purpose –

The purpose of this standard is to offer guidance for the secure configuration of Windows devices attached to the computer networks owned and operated by Salt Lake County.

Employees of Salt Lake County shall follow the *Secure Windows Device 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 Countywide information technology 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, e-mail, 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 Device
A Windows device is any workstation, laptop, tablet, phone, or device that operated the Microsoft Windows Operating system and is owned by Salt Lake County or attached to a computer network owned by Salt Lake County

3.0 Standard Guidance

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

4.0 Exceptions

Revision History
AUGUST2021 - MLE

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 policy may be subject to disciplinary action, including but not limited to temporary loss of network connectivity, loss of Internet access, or termination of access to any Salt Lake County Network and can lead to other disciplinary action, up to and including termination of County employment.

Revision History
AUGUST2021 - MLE

Appendix A
Secure Windows Device Standard

Hardware Requirements

- All hardware devices must conform to the "General IT Standards List for Purchases" published by the Information Technology Division.

Hardware and Software Inventory

- An accurate inventory of all Windows devices will be maintained.
- An accurate inventory of all software installed on Windows devices will be maintained.

Hardware Disposal

- Windows devices and peripherals that are 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.

Operating System Requirements

- All operation systems must conform to the "General IT Standards List for Purchases" published by the Information Technology Division.
- Windows operating system versions used on the County network must have supported status from Microsoft.
- Windows operating system versions no longer supported by Microsoft shall have additional security restrictions in place.
- Windows operating system versions no longer supported by Microsoft will not be allowed to connect to the Internet.
- Windows operating system versions, no longer supported by Microsoft, will not be allowed to access e-mail in any form.
- Change all default passwords before deploying any new operating system.

Imaging Requirements

- Windows devices will be imaged with an approved County agency operating system image.
- Secure images or templates shall be maintained for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or an existing system that becomes compromised should be imaged using one of those images or templates.
- Master images and templates shall be stored on securely configured systems, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
- System configuration management tools will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals or through AD group policy.

Security Configuration Settings

- Windows devices shall be joined to the County domain.
- Computer objects shall be moved to the correct OU immediately after they are joined to the County domain.
- Windows devices shall be configured with the baseline security policy through GPO.
- Mobile devices (laptops, tablets, external drives, and phones) that store or process County data shall be encrypted.
- TPM chips used for encryption purposes shall be enabled before laptops are connected to a Salt Lake County network.
- System configuration management tools will be deployed to automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.

Revision History
AUGUST2021 - MLE

- Workstations 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 that can be configured to apply protection to a broader set of applications and executables shall be deployed.

Endpoint Management Settings

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

Application Requirements

- Device owners must have a valid license for all applications used on Windows devices.
- As defined by the Information Technology Division and individual agencies, only software in the authorized software inventory will be installed or used.
- Unauthorized software shall be removed, and the inventory will be updated promptly.
- Windows devices required to run unauthorized, risky business applications shall be physically or logically segregated from other systems on the County network.

Browser and E-mail Requirements

- Only fully supported web browsers and e-mail clients are allowed.
- Windows devices should use the latest version of browsers and e-mail clients provided by the vendor.
- Browser and e-mail clients will be patched regularly.
- Any unauthorized browser or e-mail client plugins or add-on applications will be disabled.
- Only authorized scripting languages are allowed to run in web browsers and e-mail clients.

Account Configuration and Use

- The use of Windows devices will comply with County IT standards for Privileged Access Management.
- Change all default passwords before deploying any application.
- Regular user accounts will not have administrative rights on Windows devices.
- Administrator user accounts shall not be used to log in to Windows devices.
- Administrator user accounts shall not be used to run services or scheduled tasks on Windows devices.

Logging and Monitoring Requirements

- Devices must be configured to use at least three synchronized time sources to retrieve time information regularly so that timestamps in logs are consistent.
- Devices must have local logging enabled and configured to the 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 devices 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 will 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, workstation location, and duration.