SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
SECURE NETWORK CONFIGURATION

Purpose –

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

Employees of Salt Lake County are expected to follow the *Secure Network Configuration Standard* 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 the Salt Lake County Information Technology Division ("IT") to provide information technology standards. Also referencing the following:

All Countywide Information Technology Security Policies in the 1400 series
All Countywide Human Resource Policies

1.0 Scope

All Salt Lake County employees and anyone that uses a Salt Lake County provisioned network shall adhere to this Countywide information technology standard.

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.

Salt Lake County Wired Network
A wired network that uses cables to connect devices, such as laptop or desktop computers, to the Internet or another network. The most common wired networks use cables connected at one end to an Ethernet port on the network router and the other end to a computer or other device.

Salt Lake County Wireless Network
Wireless networks are computer networks that are not connected by cables of any kind. A wireless network enables enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations.

Salt Lake County Internet of Things (IoT) Network

The IoT refers to the ever-growing network of physical objects that feature an Internet Protocol ("IP") address for internet connectivity and communication between these objects and other Internet-enabled devices and systems.

Secure Administrative Workstations

Secure administrative workstations are purpose-built, secure workstations used to conduct the administration of IT resources and systems. Secure administrative workstations will only have the tools required for the administration of IT resources and systems.

3.0 Standard Guidance

All Salt Lake County employees and anyone that uses a Salt Lake County provisioned network shall follow the County's Secure Network 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 in accordance with County disciplinary policies.

Appendix A
Secure Network Configuration Standard

Salt Lake County Wired Networks

- County-owned devices that are domain members (workstations/laptops) used by County employees may use this network.
- County-owned devices that are not domain members (laptops/tablets/ipads/phones) are not allowed to use this network.
- Personal employee devices are not permitted to use this network.
- Network access is contingent on successful authentication based on computer user and device AD credentials.
- Personal use of County-owned devices on this network is covered by policy 1400-1.

Salt Lake County Wireless Networks

SLCO - Enterprise Wireless Network

- County-owned mobile devices that are domain members (laptops) used by County employees may use this network.
- County-owned mobile devices that are not domain members (tablets, ipads, phones) are not allowed to use this network.
- Personal employee devices are not permitted to use this network.
- Network access is contingent on successful authentication based on computer user and device AD credentials.
- Personal use of County-owned devices on this network is covered by policy 1400-1.

SLCO_IoT - Wireless Networks

- County-owned IoT devices requiring basic internet connectivity may use this network.
- County-owned devices that are domain members are not allowed to use this network.
- Use of this network requires:
  - A specific password and
  - A firewall update to enable access outside this network.

SLCO_GUEST - Public Access Wireless Network

- Employee or Public personal devices may use this network.
- County-owned, non-domain member devices (tablets/ipads/phones) are allowed to use this network.
- County-owned domain member devices are not permitted to use this network.
- Employee access:
  - Employees will use their Active Directory credentials to authenticate to this network.
- Public access:
  - The public will register for a 30-day passcode to authenticate to this network.

Hardware Inventory

- An accurate inventory of all wireless access points shall be maintained.
- An accurate inventory of all network devices shall be maintained.
- An accurate inventory of all network security devices shall be maintained.
- An accurate inventory of all IoT devices shall be maintained.

Hardware Disposal

Revision History
AUGUST 2021 - MLE

- Wireless access points 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.
- Network devices no longer service will be accepted with a completed PM2 form by the Information Technology Division for disposal through approved e-waste recycling programs.
- Network security devices 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.
- IoT devices 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.

Configuration Management

- IT staff will maintain and employ standard, documented security configurations for all authorized network devices.
- All configuration rules that allow traffic to flow through network devices (firewalls) should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.
- The latest stable version of any security-related updates will be installed as quickly as possible on all network devices.
- The security configuration of all network devices will be compared against approved security configurations defined for each network device in use, and an alert when any deviations are discovered will be configured and reported.
- County network devices will use at least three synchronized time sources to retrieve time information regularly so that timestamps in logs are consistent.
- County network devices will be managed using multi-factor authentication and encrypted sessions.
- Change all default passwords before deploying any network hardware.

Wired Network Security

- Port-level security is required to be implemented on all County network wired ports
- Port-level access control will follow the 802.1x standard.
- Client certificates will be used to authenticate hardware assets connecting to the County's network where ever possible.
- Port access is contingent on successful authentication based on computer user and device AD credentials.
- Other devices that do not support the traditional port-level security will be attached to ports that have been manually configured to support them using 802.1x standards.
- Protected networks will be provisioned to physically or logically segregated systems that run software that is required for business operations or that might incur higher risk for the organization
- Information Services will provision all connectivity to the Internet or business partners.
- Devices that are not approved for use on County wired networks will be immediately disabled and removed.

Wireless Network Security

- Vulnerability management systems will be configured to detect and alert when unauthorized wireless access points are connected to the wired network.
- Wireless intrusion detection systems will be configured to detect and alert when unauthorized wireless access points are connected to the network.
- Wireless access on devices that do not have a business purpose for wireless access will be disabled.
- Wireless access for client machines with an approved wireless business purpose will be configured to access only authorized wireless networks and restrict access to other wireless networks.
- Peer-to-peer (ad-hoc) wireless network capabilities on wireless clients will be disabled.
- All wireless data in transit will be protected with the Advanced Encryption Standard.

- Wireless networks must use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security.
- Devices will have all wireless peripheral access (Bluetooth and NFC) disabled unless such access is required for a business purpose.
- Separate wireless networks for personal or untrusted devices will be implemented.
- Access to "guest" networks will be treated as untrusted and filtered and audited accordingly.
- Devices that are not approved for use on County wireless networks will be immediately disabled and removed.

Logging and Monitoring Requirements

- Network devices must be configured to use at least three synchronized time sources to retrieve time information regularly so that timestamps in logs are consistent.
- Network devices must have local logging enabled and configured to the IT specifications:
  - Event source
  - Event date
  - Current user
  - Event timestamp
  - Event source addresses
  - Event destination addresses and
  - Other as specified by GPO.
- Ensure that all network devices that store logs have adequate storage space for the logs generated until they can be transferred to a central log management system.
- Ensure the collection of NetFlow and logging data on all network boundary devices.

External Network Boundary Requirements

- Information Technology will maintain an up-to-date inventory of all of the organization's network boundaries.
- Information Technology will deny communications with known malicious or unused Internet IP addresses and limit access only to trusted and necessary IP address ranges at each organization's network boundaries.
- Information Technology will deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols can cross the network boundary in or out of the network at each organization's network boundaries.
- Information Technology will configure monitoring systems to record network packets passing through the boundary at each organization's network boundaries.
- Information Technology will deploy network-based Intrusion Detection Systems (IDS) sensors to look for unusual attack mechanisms and detect these systems' compromise at each of the organization's network boundaries.
- Information Technology will deploy network-based Intrusion Prevention Systems (IPS) to block malicious network traffic at each organization's network boundaries.
- Information Technology will ensure that all network traffic to or from the Internet passes through an authenticated application layer proxy configured to filter unauthorized connections.
- Information Technology will decrypt all encrypted network traffic at the boundary proxy before analyzing the content. However, the organization may use whitelists of allowed sites to be accessed through the proxy without decrypting the traffic.
- All Virtual Private Network remote login access to Salt Lake County networks will be:
  - Provisioned by Information Technology

- Encrypt data in transit
- Use multi-factor authentication and
- IPSec connections will require that devices meet the County's *Windows Secure Device Configuration Standard.*

Internal Network Boundary Requirements

- The County's networks will be segmented based on the label or classification level of the information stored on the servers, locate all sensitive data on separated Virtual Local Area Networks (VLANs).
- Enable firewall filtering between VLANs ensures that only authorized systems communicate with other systems necessary to fulfill their specific responsibilities.
- Disable all workstation to workstation communication to limit an attacker's ability to move laterally and compromise neighboring systems through technologies such as Private VLANs or micro-segmentation.

Secure Administrative Workstations

- Secure administrative workstations are purpose-built, secure workstations used to administer IT resources and systems, including network devices, firewalls, and other security-related systems.
- Secure administrative workstations will only have the tools required to administer IT resources and systems, including network devices, firewalls, and other security-related systems.
- Secure administrative workstations will not have standard office applications, email and will not be used for general Internet access.
- A secure administrative workstation's preferred configuration is a physical machine connected to a virtual machine for regular workstation functions such as office applications, email, and public Internet access.
- Secure administrative workstations will be segmented to a dedicated, secure VLAN and will have no Internet connectivity.
- Secure administrative workstations will receive particular group policies and other controls to keep them in a pristine state.
- Scripting tools (such as Microsoft PowerShell and Python) are limited to only administrative or development users who need to access those capabilities.