SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
PRIVILEGED ACCESS MANAGEMENT

Purpose –

Privileged Access Management [PAM] is the management of computer user accounts granted administrative powers within a County information technology (IT) resource or system. These administrative powers are significantly greater than those available to regular, non-privileged computer user accounts. Failure to properly manage privileged access accounts introduces risk. The misuse of privileged access accounts is a primary method for attackers to compromise County IT resources and systems. This privileged account management standard has been developed to reduce risk to County IT resources and systems.

Employees of Salt Lake County are expected to follow the privileged access management standard established by the Information Technology Division. 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 develop 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 shall adhere to this Countywide IT standard whenever they access County IT 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

County 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.

Unprivileged User Account

Unprivileged user accounts are used for standard office applications, including email and general Internet access on a workstation. Unprivileged user accounts do not have local administrative access and are not a member of any group with local administrative access on workstations or servers.

Privileged User Account

Privileged user accounts, which, by function or security access, have been granted special privileges within County IT systems or resources, which are significantly greater than those available to the majority of users, including but not limited to, local administrative accounts, privileged user accounts, domain administrative accounts, emergency accounts, service accounts, and application accounts. Service and application accounts ideally should not have privileged permissions.

The Principle of Least Privilege

The principle of least privilege requires that a user is given no more privilege than necessary to perform an authorized job or task. Ensuring least privilege requires identifying what the user's job is, determining the minimum set of privileges needed to perform that job, and restricting the user to those privileges and nothing more. Privileges should be granted only for the timeframe required for the job. The principle of least privilege will be employed, requiring that access control permissions for all systems be set to a default that blocks access by unauthorized users. Every information system privilege that has not been specifically allowed is forbidden.

3.0 Standard Guidance

3.1 Privileged access enables an individual to take actions that may affect computing systems, network communication, accounts, files, data, or other users' processes. Privileged access is typically granted to system administrators, network administrators, staff performing computing account administration or other such information technology employees whose job duties require special privileges over a computing system or network. Individuals with privileged access must not abuse their access capability and strictly respect their functional access authority limits, respect the rights of the system users, respect the integrity of the systems and related physical resources, and comply with any relevant County policy or standard.

3.2 Privileged access may be used only to perform assigned job duties. If methods other than using privileged access will accomplish an action, those other methods must be used unless the burden of time or other resources required justifies using privileged access.

3.3 The principle of least privilege will be employed, requiring that access control permissions for all systems must be set to a default that blocks access by

unauthorized users. Every information system privilege that has not been specifically allowed is forbidden.

3.4 All County employees will follow the privileged access management standard as defined in appendix A. It is understood that this standard is best practice and should be invoked wherever possible to protect County IT resources and systems.

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 shall be subject to disciplinary action by County disciplinary policies.

Revision History
AUGUST 2021 - MLE

Appendix A
Privileged Access Management Standard

Workstation Administrator Account

- Workstation administrator accounts **will not** be used for:
  - Using office applications
  - Using email nor will they have an email address associated with them
  - General Internet access
  - For non-administrative tasks on workstations
- Workstation administrator accounts **will be** used for:
  - Administration functions on workstations
- Workstation administrator accounts will follow this format: "username-W"
- The Directory Name and Display Name fields will follow this format: "full name-W"
- The setting for "Account is sensitive and cannot be delegated" will be enabled.
- Alias usernames are not supported at Salt Lake County
- Passwords will follow the IT standard for passwords.
- Default system passwords are not allowed and must be changed.
- Employees will always use a unique password(s) for their privileged account(s) different from passwords used for all other County and personal accounts.

Server Administrator Account

- Server administrator accounts **will not** be used for:
  - Using office applications
  - Using email nor will they have an email address associated with them
  - General Internet access
  - For non-administrative tasks on workstations
- Server administrator accounts **will be** used for:
  - Administration functions on servers
  - Active Directory management
- Server administrator accounts will be created following this format: "username-S"
- The Directory Name and Display Name fields will follow this format: "full name-S"
- The setting for "Account is sensitive and cannot be delegated" will be enabled.
- Alias usernames are not supported at Salt Lake County
- It is strongly suggested that server administrator accounts only be used in conjunction with the Thycotic Secret Server privileged access system or local login to servers
- Passwords will follow the IT standard for passwords.
- Default system passwords are not allowed and must be changed.
- Employees will always use a unique password(s) for their privileged account(s) different from passwords used for all other County and personal accounts.

Domain Administrator Account

- Domain administrator accounts **will not** be used for:
  - Using office applications
  - Using email nor will they have an email address associated with them
  - General Internet access
  - For non-administrative tasks on workstations

- Domain administrator accounts **will only be used** in conjunction with the Thycotic Secret Server privileged access system.
- Domain administrator accounts will be created in the Thycotic Secret Server system following this format; "f_da*" where * is an incrementing number starting at 1.
- There should be no day-to-day user accounts in the domain administrator group except for the local Administrator account for the domain and the break-glass account.
- Membership in domain administrator groups should be required only in build or disaster-recovery scenarios.
- Passwords will follow the IT standard for passwords.
- Default system passwords are not allowed and must be changed.
- Employees will always use a unique password(s) for their privileged account(s) different from passwords used for all other County and personal accounts.

Enterprise Admin Accounts

- Enterprise administrator accounts **will not** be used for:
    - Using office applications
    - Using email nor will they have an email address associated with them
    - General Internet access
    - For non-administrative tasks on workstations
- There should be no day-to-day user accounts in the enterprise administrator group except the domain's local administrator account and the break-glass account.
- Passwords will follow the IT standard for passwords.
- Default system passwords are not allowed and must be changed.
- Employees will always use a unique password(s) for their privileged account(s) different from passwords used for all other County accounts.

Privileged Account Creation Process

- Requests for privileged accounts will be submitted through the regular access request procedure by an agency Security Authorizer. The request should include the type of privileged access requested and the reason for the privileged access.
- To ensure only authorized individuals have elevated privileges, all privileged accounts, including domain and local accounts created by Information Technology, will be documented in the inventory of privileged accounts. County agencies that create privileged accounts must also document those accounts in the inventory of privileged accounts.
- For agencies that create privileged accounts, creating a new account should be promptly communicated to the Information Security Team for tracking purposes
- All privileged accounts will avoid the use of default passwords.
- All passwords will follow the IT standard for passwords.
- Local privileged accounts will have passwords unique to the system they are provisioned for.

Use of Privileged Accounts

- Employees with privileged accounts will be responsible for safeguarding their accounts by following the rules stated in this standard.
- Privileged accounts must have a unique password that is never shared.
- Employees will not reuse passwords across County accounts and home accounts.
- If there is a reason to believe that an account has been compromised, the owner of the account will immediately notify the Information Technology Security Team.

Revision History
AUGUST 2021 - MLE

- Privileged accounts will not be used to run services or scheduled tasks on workstations or servers. Service accounts will be used where required.
- Privileged accounts will be used in conjunction with multi-factor authentication where possible.
- The management of network devices will require the use of multi-factor authentication.
- Privileged account credentials will be encrypted when in use and at rest.
- A documented process to revoke privileged access will be defined and followed.
- A documented process to disable any account that cannot be associated with an approved business process or a business owner will be defined and followed.
- A documented process to disable dormant accounts will be defined and followed.
- All temporary or vendor accounts will have a documented expiration date that is monitored and enforced.

Privileged Account Deletion Process

- When privileged access is no longer required due to termination of employment or a change in duties, the privileged accounts must be promptly disabled or deleted.
- Requests for deletion of privileged accounts should be submitted through the access request process by an agency Security Authorizer. The request should include the name of the privileged account and the date for deletion.
- The inventory of privileged accounts will be updated when accounts are deleted.

Management and Monitoring of Privileged Accounts

- Privileged accounts will be tightly managed and closely monitored by the Information Technology Security Team.
- The successful use of a privileged account will be logged on all County systems.
- The unsuccessful use of a privileged account will be logged and an alert generated on all County systems.
- All changes to administrative group membership will be logged and an alert generated on all County systems.
- If the Information Technology Security Team has reason to believe that a privileged account has been compromised, the account will be disabled.
- If the Information Technology Security Team has reason to believe that a privileged account is not being used, the account will be disabled, and the owner of the account may be subject to disciplinary action.
- Privileged accounts used to perform penetration testing should be controlled and monitored to ensure they are only being used for legitimate purposes and are removed or restored to normal function after testing is over.

Secure Administrative Workstations

- Secure administrative workstations are purpose-built, secure workstations used to conduct the administration of County IT resources and systems.
- Secure administrative workstations will only have the tools required for the administration of County IT resources and systems.
- Secure administrative workstations will not have standard office applications, email and will not be used for general Internet access.
- The preferred configuration of a secure administrative workstation is a physical machine, with a connection to a virtual machine for regular workstation functions such as office applications, email, and general Internet access.
- Secure administrative workstations will be segmented to a dedicated, secure VLAN and will have no connectivity to the Internet.

- Secure administrative workstations will receive special group policies and other controls to keep them in a pristine state.
- The use of scripting tools (such as Microsoft PowerShell and Python) is limited to only administrative or development users who need to access those capabilities.