SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
REGULAR AND SERVICE ACCOUNTS

Purpose –

The purpose of this standard is to provide guidance and simplify the lifecycle of regular and service accounts used to access County information technology (IT) resources or systems. This lifecycle includes the proper creation, maintenance, and retirement of these accounts. Regular and service accounts are typically used for access to specific County IT resources and systems. These accounts will not normally have administrative access to the system on which they are used.

Employees of Salt Lake County are expected to follow the regular and service account 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 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.

Regular User Accounts
A regular user account is typically the account most employees use for day-to-day work like logging onto a computer, accessing email, or accessing the Internet. Therefore, regular user accounts should not have any special permissions that could potentially lead to damage

or data loss. In addition, regular user accounts should not have administrative access to any County IT resource or system.

Service Accounts

A service account is a special user account that an application or service uses to interact with the operating system. For example, services use these service accounts to log on and make changes to the operating system or the configuration. Through permissions, you can control the actions that the service can perform.

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 requires 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 Regular user accounts are the most common type provisioned for County employees. This type of account will not have administrative access to any County IT resource or system. Instead, this type of account will be used to access email, access the Internet, and most of the tasks a County employee performs in a typical day. County employees shall never share the password for their regular user account. Instead, employees will choose a unique password for their regular user account different from the password used for all other County accounts (if applicable).

3.2 Shared user accounts are provisioned on a limited basis. These accounts are typically used at front counters or kiosks. These accounts will not have administrative access to any County IT resource or system. Additionally, this type of account will not be provisioned for email. Commonly, more than one County employee will know the password for this type of account. For this reason, these accounts should not have access to the Internet except for specific work-related purposes as there is an inherent lack of accountability.

3.3 A current County employee must request any account defined in this standard that is provisioned for a non-County employee. This employee will be considered the sponsor for the non-County employee. The requesting County employee will, in their role as sponsor, monitor the use of the account. These accounts, except for volunteers, will have a pre-determined expiration date. Continued use of the

account will require the sponsoring County employee to verify that access is still needed.

3.4 The accounts defined in this standard are created for specific purposes. Therefore, county employees will only use them for those specific purposes. Misuse of these accounts will be considered a violation of the County's Acceptable Use Policy.

3.5 The principle of least privilege will be employed, requiring that access control permissions for all systems must be set to a default which blocks access by unauthorized users, and every information system privilege which has not been specifically allowed is forbidden.

3.6 All County employees will follow the regular and service account 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 or systems.

4.0 Exceptions

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

5.0 Enforcement

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

Appendix A
Regular and Service Account Standard

Regular User Account

- Purpose: Default un-privileged user account for workstation and network access
- Convention: [first initial] [last name]
    - Example: PSmith
- Add the user's middle initial or additional letters from the user's first name to the account name for duplicate accounts.
    - Example: PLSmith or PeSmith
- The account will be assigned to a single user.
- The password will only be known by the assigned user.
- The password will follow the IT standard for passwords
- The password must be different from the password used for all other County accounts (if applicable).
- The account will not have administrative access to any system.
- The account may or may not have an associated email box.
- The account must use VPN/MFA to authenticate to any County information technology resource or system from off-network.

Shared User Account

- Purpose: "Generic" non-privileged user account for use by multiple people on a shared workstation
- Convention: GEN-[descriptive name]
- Example: GEN-[JLSorensen-FD1]
- The account will be assigned to a computer or group of computers.
- The password may be known by more than one employee.
- The password will follow the IT standard for passwords.
- The account will not have administrative access to any system.
- The account may or may not have an associated email box.
- The account will not be used to authenticate to any County information technology resource or system from off-network.
- The account will not be used for VPN access.

Vendor User Account

- Purpose: Account for use by a single vendor representative
- Convention: [first initial] [last name]-VEN
- Example: PSmith-VEN
- The account will be assigned to a single user.
- The password will only be known by the assigned user.
- The password will follow the IT standard for passwords.
- The account may have administrative rights to a limited number of systems.
- The account may not have an associated email box.
- The account will only be active while the vendor is using it.
- The use of the account will be closely logged and monitored.
- The account must be documented in the inventory of vendor user accounts list and the name of the County employee who is "sponsoring" the access.
- Remote access for vendor accounts will "time-out" every 30-days.
- The "sponsor" will need to verify that continued access is required.

Contractor/Consultant User Account

- Purpose: Account for use by a single contractor or consultant

Revision History
FEB 2022

- Convention: [first initial] [last name]-CON
    - Example: PSmith-CON
- The account will be assigned to a single user.
- The password will only be known by the assigned user.
- The password will follow the IT standard for passwords.
- The account may have administrative rights to a limited number of systems.
- The account may not have an associated email box.
- The account will only be active while the contractor/consultant is using it.
- The use of the account will be closely logged and monitored.
- The account must be documented in the inventory of contractor/consultant user accounts and the name of the County employee who is "sponsoring" the access.
- Remote access for contractor and consultant accounts will "time-out" every 30-days.
- The "sponsor" will need to verify that continued access is required.

Other Non-Employee User Accounts

- Purpose: User accounts for non-County / non-WFWRD / non-UPD employees
- Convention:
    - Volunteer: [first initial] [last name]-VOL
    - Intern: [first initial] [last name]-INT
    - Other non-County accounts (like CJAC): [first initial] [last name]-NC
- The account will be assigned to a single user.
- The password will only be known by the assigned user.
- The password will follow the IT standard for passwords.
- The account will not have administrative access to systems.
- The account may or may not have an associated email box.
- The account will only be active while the non-employee is using it.
- The use of the account will be closely logged and monitored.
- The account must be documented in the inventory of non-County-employee user accounts and the name of the County employee who is "sponsoring" the access.
- Remote access for non-employee accounts will "time-out" every 30-days.
- The "sponsor" will need to verify that continued access is required.

Managed Service Account

- Purpose: Account for use on a single system to run a service or application pool
- Convention: MSA [type][system]
    - Example: MSApsAF2K (managed service account for PeopleSoft AppFin2-k server)
- The account will be for use on a single system.
- The password will be managed and updated automatically by the domain.
- The password will follow the IT standard for passwords.
- The account may or may not have administrative access to the system.
- The account will not have an associated email box.
- The account will not be used to log on to a system.
- The account must be documented in the inventory of managed service accounts.

Group Managed Service Account

- Purpose: Account for multiple systems to run a service, application pool, or scheduled task.
- Convention: gMSA[type][system]
    - Example: gMSAsqlTaxProd (group managed service account for SQL Tax production system)
- The account will be for use by an application on multiple systems.
- The password will be managed and updated automatically by the domain.

- The password will follow the IT standard for passwords.
- The account may or may not have administrative access to the system.
- The account will not have an associated email box.
- The account will not be used to log on to a system.
- The account must be documented in the inventory of group-managed service accounts.

Application Service Account

- Purpose: Account for use on systems and with applications that don't support MSAs or gMSAs.
- Convention: SVC-[system]
    - Examples: SVC-NessusScan, SVC-HPLogger
- The account will be for use by a service or application on one or more systems.
- The password will be documented in Secret Server.
- The password will follow the IT standard for passwords.
- Ideally, the account will not have administrative access to systems.
- The account may or may not have an associated email box.
- The account will not be used to authenticate to any County information technology resource or system from off-network.
- The account will not be used for VPN access.
- The account must be documented in the inventory of application service accounts.

Resource Account

- Purpose: Account associated with an Exchange resource mailbox
- Convention: RS-[org]-[resource]
    - Examples: RS-IS-RoomS-3623, RS-IS-TrainCart
- The account will be for use by an Exchange resource mailbox.
- The account will not have administrative access to systems.
- The password will be documented in Secret Server.
- The password will follow the IT standard for passwords.
- The account must have an associated email box.
- The account will be disabled.
- The account will not be used to authenticate to any County information technology resource or system from off-network.
- The account will not be used for VPN access.
- The account must be documented in the inventory of resource accounts.

System Test Accounts

- Purpose: Account for use in testing a system
- Convention: TST-[system]
    - Example: TST-AntivirusTesting
- The account will not be assigned to a single user.
- The password may be documented in Secret Server.
- The account will not have administrative access to systems.
- The account may or may not have an associated email box.
- The account will not be used to authenticate to any County information technology resource or system from off-network.
- The account will not be used for VPN access.
- The account will be disabled when it is not in use.
- The account must be documented in the inventory of system test accounts.

Personal Test Accounts

- Purpose: Account for use in testing
- Convention: [first initial] [last name]-T
    - Example: PSmith-T
- The account will be assigned to a single user.
- The password will only be known by a single user.
- The password will follow the IT standard for passwords.
- The password must be different from the password used for all other County accounts (if applicable).
- The account will not have administrative access to County resources or systems.
- The account may or may not have an associated email box.
- The account will not be used to authenticate to any County information technology resource or system from off-network.
- The account will not be used for VPN access.
- The account will be disabled when it is not in use.
- The account must be documented in the inventory of personal test accounts.

Account Creation Process

- Requests for regular and service accounts will be submitted through the access request procedure by an agency Security Authorizer. The request should include the type of account and access requested.

- Requests for vendor, contractor, or non-County employee account must be accompanied by the name of the sponsoring County employee. In addition, please include a description of the purpose of the account. All accounts of this nature must be documented in the inventory of vendor, contractor, and non-County employee accounts.

- The name of the associated system must accompany requests for service accounts. The request should also include the name of the County employee responsible for the account. Service accounts must be documented in the inventory of service accounts.

Account Termination Process

- Requests to terminate regular and service accounts will be submitted through the access request procedure by an agency Security Authorizer. The request should include the name of the account and the date the account will be terminated. Any email or data associated with the account will be deleted in 30-days unless a litigation hold is in place.

- Requests to terminate vendor, contractor, or non-County employee accounts will be submitted through the access request procedure by an agency Security Authorizer. The request should include the name of the account and the date the account will be terminated. Any email or data associated with the account will be deleted in 30-days unless a litigation hold is in place.

- Accounts on litigation hold will not be terminated until the Director of Information Security has archived all user-created data. This will include the data in any associated email accounts and any associated data on network storage devices. The account may be terminated after the Director of Information Security gives the authorization to do so.