SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
PASSWORDS

Purpose –

This standard aims to provide guidance and simplify the lifecycle of passwords used to access County IT resources and systems. This lifecycle includes the creation and maintenance of passwords. This standard encourages the use of the new concept of secure passphrases. Passwords for regular user and service accounts will not require frequent rotation except where compromise of the account is a concern. Privileged account passwords will continue to require periodic rotation.

Employees of Salt Lake County are expected to follow the password standard established by the Information Service 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 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 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, 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.

Password
A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in conjuncture with a username; they

are designed to be known only to the user and allow them to access a device, application, or website.

Privileged User Account
An account which, by function and security access, has 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

Regular User Accounts
A regular user account is a standard user account used for day-to-day work like logging onto a computer, reading email, or accessing the Internet. 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 particular user account that an application or service uses to interact with the operating system. For example, services to employ the 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 the least privilege requires identifying the user's role, determining the minimum set of privileges needed to complete that job, 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 All County users will follow the County password standard.

3.2 Any account created for use on any County IT resource or system must have a password that adheres to this password standard.

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.

Appendix A
Password Standard

User and Service Accounts		
Topic	County	Requirements
Minimum Length	15	None
Maximum Length	32	None
Password Age	1-day	None
Password History	6	None
Accept spaces	Yes	None
Character set	ASCII	None
Password hints/prompts	No	None
Password throttling	30 min. lock/5 fails/2-hours	Windows Fine-grained policy
Composition Rules	No complexity - Blacklist	nFront - dictionary
Dictionary	None	None
Repeating Characters	No more than 2 repeating	nFront
Password Display	Yes	None
Password change frequency	None unless compromised	None
Password Uniqueness	Must be different from password of all other County accounts	None

Privileged Access Accounts		
Topic	County	Requirements
Minimum Length	15	None
Maximum Length	32	None
Password Age	1-day	None
Password History	6	None
Accept spaces	Yes	None
Character set	ASCII	None
Password hints/prompts	No	None
Password throttling	30 min. lock/5 fails/2-hours	Windows Fine-grained policy
Composition Rules	No complexity - Blacklist	nFront - dictionary
Dictionary	None	None

Repeating Characters	No more than 2 repeating	nFront
Password Display	Yes	None
Password change frequency	a password will be changed every 120-days	None
Password Uniqueness	Must be different from password of all other County accounts	None