SALT LAKE COUNTY
COUNTYWIDE INFORMATION TECHNOLOGY STANDARD
ON
ROLE-BASED ACCESS CONTROL – GROUP NAMES

Purpose –

Role-Based Access Control [RBAC] is the management of access to resources based on roles. The County will realize several benefits from using RBAC, including:

- Improving operational efficiency
  With RBAC, assigning the proper rights for new hires or role changes in existing employees will be easier. It can also make scripting easier where user roles are involved.
- Increased visibility for administrators
  RBAC will make it easier for administrators to know what a user has access to.
- Reducing costs
  Clarifying the roles and associated privileges will lessen the time spent understanding and communicating the proper configurations for user accounts. It will also help ensure that resources are only used by the appropriate individuals and potentially decrease licensing and infrastructure resources.
- Decreasing risk of breaches and data compromise
  RBAC restricts access to sensitive information, reducing the potential for data compromise. Managing accounts using RBAC will help ensure compliance with "Principle of Least Privilege" standards is met.

The Salt Lake County Information Technology Division employees are expected to follow the role-based access control standard - group names standard established by the Information Technology Division. The Information Technology Division will monitor and enforce compliance with this standard.

Reference –

The policy and standards set forth herein are provided in accordance with Section 3.10 of Countywide Policy 1400, which directs Salt Lake County Information Technology to provide security systems and policies. 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 Information Technology Division employees shall adhere to this Information Technology Division policy 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.

Revision History
DEC 2019 - MLE

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.

Role-based Access Control
Role-based access control is an approach to restricting access to authorized users based on their role or job function within the organization.

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 what the user's role 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.

Role Groups
Role groups are Active Directory groups that represent a role or responsibility. These usually tie to a job role or task that the user performs.

Permission Groups
Permission groups are assigned access to a single resource and access level. If a resource needs to have multiple access levels assigned to it, separate permission groups will need to be created and assigned to each level.

Permission groups contain only Role groups and special user accounts such as service accounts.

3.0 Policy Statement

3.1 Roles will be defined with permissions restricted only to what is required for the associated function.

3.2 Decisions for determining what permissions will be included for a particular role and included in each role group will be made by the Associate Director or manager who oversees the role.

3.3 Access to resources will only be defined by inclusion in Role Groups wherever possible.

3.4 All Information Technology Division employees will follow the role-based access control standards as defined in Appendix A of this policy where possible. It is understood that this standard is best practice and should be invoked where ever possible to protect County IT resources and systems.

4.0 Exceptions

Any exceptions to this policy 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 shall be subject to disciplinary action by County disciplinary policies.

APPENDIX A
ROLE-BASED ACCESS CONTROL – GROUP NAME STANDARD

Permissions Groups

- Permissions Groups will be defined in the slcounty.org\Domain Groups OU
- Permissions Groups will contain only Role Groups
- Naming standards Permission Groups will use the following convention:
  P-<division abbreviation>**-**<resource>**-**<access level>
  Ex: P-BH-DataWarehouse-Read
- A separate Permissions Group will be created for each resource/access level combination.

Role Groups

- Role Groups will be defined in the slcounty.org\Domain Groups OU
- Naming standards for Role Groups will use the following convention:
  R-<division abbreviation>**-**<role>
  Ex: R-BH-DataWarehouseUser
- Role Groups will be used whenever possible for assigning permissions to resources
- Users will be added directly to Role Groups, but not Permissions Groups.
- Built-in Roles (such as Domain Users) can be leveraged where it makes sense.

Role-Based Access Group administration

- Role-Based Access Groups will be created, modified, and deleted by account administrators in the Information Technology division and other divisions that administer their accounts.

Revision History
AUGUST 2021 - MLE