

User Account Management Policy

# Overview/Purpose

User Accounts control access to <**Utility Name**>'s technology resources, including networks, systems, and software applications. The proper creation, control, and supervision of all User Accounts is vital to <**Utility Name**>'s security and ability to maintain its operations.

The purpose of this policy is to establish a formal process to ensure that User Accounts are appropriately created, securely used, and terminated as required in a timely fashion. This policy is necessary to safeguard the confidentiality and integrity of <**Utility Name**>'s information, and to protect its customers.

# Scope

All employees, contractors, consultants, temporary and other workers at <**Utility Name**> and its subsidiaries must adhere to this policy. This policy applies to IT systems that are owned, operated, or leased by **<Utility Name>** or registered under a company-owned network domain.

# Policy

## General

The <**person or group responsible for policy**> is responsible for ensuring that this policy is adhered to. All authorized users will be provided one or unique User Accounts for their sole use. All such accounts must be uniquely identifiable by an assigned user name. All accounts must have a password that complies with the*Password Policy*.

### Individual Accounts

Individual, named accounts are required when accessing IT resources. Users are accountable for their actions, which can be reviewed via audit trails maintained by the systems to which they have access rights. Individual users must adhere to the terms and conditions of the *Acceptable Use Policy*.

### Administration (Privileged) Accounts

IT Administrative staff can be granted privileged accounts that permit elevated access rights for specific systems and/or applications, as needed for support and maintenance. Generic/built-in privileged accounts (e.g. Windows domain and local administrator, etc.) shall not be used for daily systems administration. A named, privileged account must be used instead.

### Application-Specific Accounts

An application-specific account controls access to an individual application Access rights and privileges are configured within each application. These accounts will typically have the same name as the user's primary account.

### Guest/Group Accounts

Guest/group accounts are not permitted on **<Utility Name>**'s systems or applications. All users, permanent or temporary, must have a unique, named account.

## Account Creation

### New employee account

When a new employee is hired, the hiring Manager will submit an *IT Employee Change Form* which specifies the Organizational Role of new employee. Based on the Organizational Role, the IT Department will create permissions using Role Based Access Control (RBAC) procedures, and a unique temporary password.

A user is not permitted, under any circumstances, to inherit a User Account that was originally assigned to another user. Before access is given to an account, all users should be provided with the **<Utility Name>** Acceptable Use Policy. {Or any other policy that might pertain to using the Coop’s IT resources}

### New software applications

While implementing a new application, the IT Department will create an RBAC structure in coordination with system owner. User Accounts for the new system shall be added based on the new RBAC structure.

## Account Deletion

A user’s manager must immediately notify IT or HR. of changes in a user’s employment status (departure, extended leave) and submit *IT Employee Change Form*. The IT Department will then immediately disable or remove all associated User Accounts.

## Account Management

The IT Department will:

* Ensure that disabled User Accounts are not re-issued to another user.
* Leave the associated User Account disabled for 30 days to facilitate the disposition of files or other resources assigned to the Account. (The User Account will be deleted after 30 days).
* Modify User Accounts in response to events like name changes, accounting changes, permission changes, or office transfers.
* Remove, after consultation with a user’s manager, redundant User Accounts that are no longer required.
* Periodically review existing User Accounts for validity.
* Grant Supervisors access to an account if an employee is involuntarily removed from a position to ensure continuity of communication for business purposes. Also, upon special request, a supervisor will be granted access to the account after an employee voluntarily terminates their employment.

# Compliance

## Compliance Measurement

The <**person or group responsible for policy**> will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

## Exceptions

Any exception to the policy must be approved, in writing, by the <**person or group responsible for policy**> in advance.

## Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action in accordance with **<Utility Name>** HR policies.

# Related Standards, Policies, and Processes

* Adapted from “Cyber Security Policy Framework” (<https://www.nreca.coop/wp-content/uploads/2015/09/cyber_security_policy_framework.docx>)   
  Cyber Security Policy Framework was created by the Kentucky Association of Electric Cooperatives (KAEC) Information Technology (IT) Association - Cyber Security Subcommittee.
* Adapted from SANS , “Inventory of Authorized and Unauthorized Devices” (<http://www.sans.org/critical-security-controls/control/1>) and “Inventory of Authorized and Unauthorized Software” (<http://www.sans.org/critical-security-controls/control/2>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| IT Manager | **CEO/GM** | **CFO**  **COO**  **Legal Department** | **All Employees** |

*[Explanatory Note: <Utility Name> should feel free to alter section to reflect the specific responsibility requirement determined by <Utility Name> management.]*

# Approval

\_

<**Insert title of approver**> Date

# Revision History

|  |  |  |
| --- | --- | --- |
| Date of Change(s) | Revised by | Summary of Change(s) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |