

Password Policy

# Overview/Purpose

Passwords are an important aspect of computer security. A poorly chosen password may result in unauthorized access and/or exploitation of <**Utility Name**>'s resources. All users, including contractors and vendors with access to <**Utility Name**> systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

# Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides in any <**Utility Name**> facility, or is used to conduct company business.

# Policy

## Password Creation

* + 1. All user-level and system-level passwords must conform to the Password Construction Guidelines.
    2. Users shall never use the same password for an account that is used for other non-company access (for example, personal ISP account, option trading, benefits, etc.).
    3. Excluding Single Sign-On, users must not use the same password for multiple systems.
    4. User accounts that have administrator/system-level privileges must have a unique password from all other accounts held by that user.
    5. All default passwords must be changed on any devices before they are installed at a <**Utility Name**> facility.
    6. All User Accounts will be created with a random, single-use password. The user will be required to change the password at their first login.

## Password Change

* + 1. All system-level passwords (for example, root, enable, application administration accounts, etc.) must be changed on a reasonable periodic basis.
    2. All user-level passwords (for example, email, web, desktop computer, etc.) must be changed at least every 90 days.
    3. Password cracking or guessing audits may be performed on a periodic or random basis by the <**person or group responsible for policy**>. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the *Password Construction Guidelines*.
    4. Password changes may be required upon identification or notification of a cybersecurity incident or threat.  
         
       **[If utility is processing credit cards, passwords should be changed every 90 days to satisfy PCI DSS requirements]**

## Password Protection

* + 1. Passwords must not be shared with anyone, including administrative assistants, secretaries, managers, co-workers while on vacation, IT, and/or family members.
    2. Passwords must not be inserted into email messages or other forms of electronic communication.
    3. Passwords must not be revealed over the phone to anyone.
    4. Passwords must not be revealed on questionnaires or security forms.
    5. Hints should never be provided as to the format of a password (for example, "my family name").
    6. Passwords must not be written down or stored anywhere in an office, home, or any other location. Passwords must not be stored in a file on a computer system or mobile devices (phone, tablet) in clear text.
    7. The "Remember Password" feature of applications must not be used (for example, web-based systems).
    8. Any user suspecting that his/her password may have been compromised must report the incident to <**person or group responsible for policy**>, and change all passwords immediately.

## Storing passwords

<**Utility Name**> may provide their employees with a password vaulting or identity management system for storing passwords to different systems. Password for accessing these programs shall use the same rule for password structure. Employee may be permitted to store also their personal passwords in such a system, but access to that system cannot be shared.

# 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 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 “Password Protection Policy”  
  (<http://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>)
* PCI DSS Requirements  
  (<https://www.pcisecuritystandards.org/document_library>)

# Governance Responsibilities

The ISP uses the RACI model for assigning responsibility.

|  |  |  |  |
| --- | --- | --- | --- |
| Responsible | Accountable | Consulted | Informed |
| CIO | **CEO/GM** |  | **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) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |