October 2023

Identity Security Policy │ Policy

POLICY OWNER:	Technology Department
POLICY APPROVED BY:	Chief Operating Officer & Director, Human Resources.
POLICY CONTACT:	Technology Department, help@water.org Director of Technology, kbridges@water.org

Policy Contents

I. Policy Overview

Policy Statement

This policy is to establish acceptable security measures for user identification within Water.org managed systems.

Purpose

The purpose of this policy is to establish acceptable security measures for user identification within Water.org managed systems.

Applicability

This policy applies to all enterprise digital solutions used within Water.org and all personnel, third party contractors, guests, or anyone else who uses, possesses, or has access to Water.org systems and applications.

Governance

The **Technology Department** is the owner of this policy and is responsible for administering, reviewing, and making recommendations for updates or changes to this policy in alignment with business needs.

Violations

It is the expectation of Water.org that direct supervisors proactively manage their direct reports' compliance with this Policy. Non-compliance, from an employee or a direct supervisor, may result in progressive disciplinary actions consistent with the organization's established HR procedures.

II. Policy

1. Administration

- All user-level and system-level passwords must conform to the guidelines described below.
- All local accounts (in the system) must conform to the guidelines described below.

2. Requirements

Some of the more common uses of passwords include user level accounts, web accounts, email accounts, screen saver protection, and voicemail password.

Weak passwords have the following characteristics:
- The password contains less than eight (8) characters
- The password is a word found in any language (English, non-English, slang, jargon, proper nouns, etc.)
- The password is a common usage word such as:
  - Names of family members, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aabbccdd, qwerty, zyxwvuts, 12344321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
  - Any of the above with some letters substituted (like passw0rd)

Strong passwords have the following characteristics:
- Contains both upper-case and lower-case characters (e.g., a-z, A-Z)
- Contain numbers (0-9).
- It contains at least eight characters.
- Is not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase.
- Passwords should never be shared with anyone for any reason, except when required by the IT team to do remote maintenance of laptops. If an issue or situation arises that requires you to share your password, immediately change it at the first opportunity.

3. Password Management

Do not share Water.org passwords with anyone, except when required by the IT team to do remote maintenance of laptops. If an issue or situation arises that requires you to share your password, immediately change it at the first opportunity. All passwords are to be treated as sensitive, confidential information.

Here is a list of "do not":
- Do not reveal a password over the phone to ANYONE
- Do not use a password that is the same or like one you use on any other websites.
- Do not reveal a password in an email message
- Do not reveal a password to your boss
- Do not talk about a password in front of others
- Do not hint at the format of a password (e.g., "my family name")

- Do not reveal a password on questionnaires or security forms
- Do not share a password with family members
- Do not reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the IT Department.
Do not use the "Remember Password" feature of applications (e.g., Microsoft Internet Explorer, Microsoft Outlook, Mozilla Firefox, Netscape Messenger, etc.).
If you suspect an account or password has been compromised, report the incident to IT and change all passwords.
IT Security may perform password cracking or guessing on a periodic or random basis. If a password is guessed or cracked during one of these scans, the user will be required to change it. Password cracking and guessing are not to be performed by anyone outside of IT Security or by an approved 3rd party auditor.

4. Account Lockout
After five (5) consecutive failed login attempts within two (2) hours, the account is locked for fifteen (15) minutes.

5. Multifactor Authentication
Water.org staff members must establish a secondary method of authentication beyond just User ID and password authentication. This is typically achieved by using a secondary device, such as a mobile phone, and receiving a code via text message or a phone call. Additionally, an MS Authentication App can be installed on the mobile device and used to approve access.

4 Approval and Responsibility

Employee Responsibilities

It is the employee's responsibility to follow the requirements outlined above to limit any vulnerabilities and maintain a safe environment.

5 Additional Resources

Contact for Support

You may ask questions to the Technology Department, help@water.org. For more personal or confidential questions or information please contact the Director of Technology, kbridges@water.org.