October 2023

Cybersecurity Awareness and Training 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

In today's world much of our business is conducted online, it is vast and growing. The more we rely on technology to collect, store, and manage information, the more vulnerable we become to severe security breaches. A cyber-attack does not only directly threaten our organization's confidential data, but it may also ruin the relationships with customers, and cause severe legal jeopardy to them and our organization's reputation. Effective cyber security also requires the awareness and proactive support of all staff, supplementing and making full use of the technical security controls.

Purpose

This document outlines our guidelines and provisions for preserving the security of our data and technology infrastructure through proper cyber security training and testing.

Applicability

This policy applies to all Water.org employees, contractors, volunteers remote or onsite, and anyone who has permanent or temporary access to our systems.

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.

All employees will be provided with cyber-security training, and all employees will be expected to follow this policy. Should an employee disregard this policy and cause security breaches they will be subject to disciplinary action, up to an including termination.

II. Policy

1. Requirements

All awareness training must fulfill the requirements for the security awareness program as listed below:

1.1 The cyber security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of cyber security matters, such as general obligations under various cyber security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior.

1.2 Additional training is appropriate for staff with specific obligations towards cyber security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security, and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, and anticipated job requirements.

1.3 Security awareness and training activities should commence as soon as practicable after staff joins the organization, through attending cyber security induction/orientation as part of the on-boarding process. The awareness activities should continue periodically (yearly) thereafter to maintain consistent awareness.

1.4 Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why cyber security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff.

1.5 The organization will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of cyber security matters.

2. Policy Elements

The organization has outlined security measures that may help mitigate cyber security risks.

2.1 Confidential Data:

Confidential data is information for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the Organization, partners, affiliates, and customers. Common examples are:

a. Unpublished financial information
b. Credit Card Numbers
c. Data of customers/partners/vendors
d. Human resources records
e. Patents, formulas, or new technologies
f. Data security is the responsibility of all employees

2.2 Protect personal and Organization devices

a. We advise our employees to keep both their personal and Organization-issued equipment and devices secure.
b. Here is how:
    a. Use strong (numbers, letters, and symbols) passwords on all devices. (ii) Avoid opening email attachments or clicking links.
    b. Be suspicious of clickbait titles (e.g., offering prizes or gift cards, advice.)
    c. Choose and upgrade complete antivirus software.
    d. Never leave devices exposed or unattended.
    e. Do not give out personal information on the phone or through email or text.
    f. Install security updates of browsers and systems monthly or as soon as updates are available.
    g. Log into Organization accounts and systems through secure and private networks only.
    h. When you use a shared computer or a business's Wi-Fi connection, you do not know how secure the network really is. Use your own device and secure network when possible.

2.3 Managing Passwords Properly

a. Passwords are the first line of defense against numerous internet attacks of the Organization data infrastructure; hence password leaks are dangerous. Passwords should be SS, secure and secret.
b. Follow our Technology Email Address Naming and Use Policy defining naming and password specifics

2.4 Transfer Data Securely

Transferring data introduces security risk. Employees must:

a. Avoid transferring sensitive data, if information must be transferred it must first be encrypted by manager or IT specialist.
b. Confidential data must only be shared over the Organization network/ system and not over public Wi-Fi or private connection.
c. Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
d. Store data in a shared drive that only authorized persons can access.
e. Employees must report seeming attacks, suspicious emails, fraud attempts or phishing attempts as soon as possible following our Technology Security Incident Handling Policy.

2.5 Additional Measures

To mitigate the possibility of security breaches, here are some additional defenses:

a. Lock screens and devices when leaving desks.
b. Report stolen or damaged equipment as soon as possible to Technology and HR.
c. Change all account passwords when a device is stolen or compromised.
d. Report a perceived threat or security weakness in Organization systems.
e. Do not download suspicious, unauthorized, or illegal software on Organization equipment.
f. Mark any suspicious emails as “Spam” or “Phishing” within MS Outlook.
g. Avoid accessing suspicious websites.
h. We also expect our employees to comply with our social media policy.
i. Our Network Administrators should:
    a. Install Organization approved firewalls, anti-malware software and access authentication systems.
    b. Arrange security training for all employees.
    c. Inform employees regularly about new scam emails or viruses and ways to combat them.

d. Investigate security breaches thoroughly.
    i. Follow this policies provisions as other employees do.

3. Water.org Cyber security or Cybersecurity Awareness Training & Testing

Water.org Technology department requires that each employee and contractor or consultant upon hire and at least annually thereafter successfully complete basic cyber-security awareness training. Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will be given reasonable time to complete each course so as not to disrupt business operations.

3.1 Simulated Social Engineering Exercises

Water.org Technology department will conduct periodic simulated social engineering exercises/testing including phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The Technology department will conduct these tests at random throughout the year with no set schedule or frequency. Any staff member who fails one of these attack simulations will be enrolled in additional and mandatory cyber awareness training. Repeat failure to recognize test emails as fraud/phishing will be escalated to HR and management.

3.2 Remedial Training Exercises

From time-to-time Water.org staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the Water.org Technology department as part of a risk-based assessment.

4 Approval and Responsibility

Employee Responsibilities

It is the employee's responsibility to complete the annual training and stay relevant with the new tactics and take the necessary steps and cautions to limit cyber vulnerabilities.

Direct Supervisor Responsibilities

It is the direct supervisors' responsibility to ensure that their team members complete the required annual training and communicate any vulnerabilities or changes.

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.

Related Policies

Email Address Naming and Use Policy
Identity Security Policy
Technology and Computer Use Policy