

October 2023

## Security Incident Handling Policy and Procedure | Policy

<b>POLICY OWNER:</b>	Technology Department
<b>POLICY APPROVED BY:</b>	Chief Operating Officer & Director, Human Resources.
<b>POLICY CONTACT:</b>	Technology Department, <a href="mailto:help@water.org">help@water.org</a> Director of Technology, <a href="mailto:kbridges@water.org">kbridges@water.org</a>

### Policy Contents

- I. [Policy Overview](#)
- II. [Policy](#)
- III. [Approval and Responsibilities](#)
- IV. [Additional Resources](#)

### I. Policy Overview

#### Policy Statement

This policy outlines the security incident handling procedures, including the steps needed to report, categorization levels, types, and resolution steps.

#### Purpose

This policy establishes a standard for alerting appropriate personnel related to technology and data security incidents. The Technology Department will assist with remediating the issue and communicate with the proper authorities. A summary log of all incidents, resolutions, and related documentation will be maintained by the Technology Department.

#### Applicability

This policy applies to all Water.org systems, SaaS, and technology tools.

#### 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.

It is required that all users report any potential security incidents as soon as practically possible. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

## II. Policy

### 1. Incident Reporting

Users should immediately report unauthorized disclosures or uses of confidential information, as well as other potential information security incidents involving yourself or other users, to the Technology Department and to their direct manager/supervisor, or HR, or other senior Management. Personnel may report allegations without fear of retaliation and elect to remain anonymous. Potential security incidents involving Information Technology systems and equipment will be logged and tracked by the IT Department.

Potentially sensitive incidents include, but are not limited to:

- Security breaches of Water.org systems, whether resulting in the loss of Water.org confidential information, intellectual property, or other highly sensitive information
- Significant instances of misuse or misappropriations of computer assets and systems
- Thefts of Water.org hardware (e.g., Laptop) and data devices (e.g., USB or Hard Drive)
- Sensitive security issues relating to, or involving, Water.org Executives
- Situations requiring forensic analysis/investigation of Water.org computing assets
- Any situation which may pose a serious threat to Water.org's IT business processes and potentially impact on the Water.org's ability to continue operations or service its customers

Methods to Report to the Technology Department

- Initial notification/alert should be emailed to [help@water.org](mailto:help@water.org)
- If request is not immediately addressed and appropriate calls to the respective people in this order:
  - Kevin Bridges +1 816 674 6294
  - James Boomer +1 816 674 5355
  - Jennifer Riddle +1 816 301 5131
  - Atman Walters +1 816 898 3594

### 2. Incident Severity

Classifying the severity of each security incident helps technology personnel and management determine the appropriate course of action including escalation. Each incident will be classified by the Technology Department, HR, Legal and/or executive management as one of the following:

- **Critical Severity** – incident may involve critical data, serious legal issues, service disruption impacting all operations, financial loss, an active threat, and/or involves damaging public interest.
- **Sensitive Severity** – incident may involve sensitive data, less serious legal issues or potential for legal issues, service disruption impacting a location, potential for disrupting operations, potential threat, somewhat widespread, and/or potential for damaging public interest.
- **Low Data Severity** – incident involving unrestricted data, may not involve any legal issues, low potential for service disruption, low risk of threat, limited reach and/or low damaging public interest.

### 3. Resolution

Technology personnel administering security will confer on the referred matter as soon as possible to identify the potential risks/exposure and potential responses. The Water.org Technology personnel

administering security will engage Legal, Senior Management, Human Resources, and other internal resources in determining the appropriate course of action.

A summary log of all incidents, resolutions, and related documentation will be maintained by the Technology Department.

#### **4 Approval and Responsibility**

##### **Employees Responsibility**

Employees and/or their managers are responsible for immediately notifying the Technology Department ([help@water.org](mailto:help@water.org)) regarding a potential security incident.

##### **Technology Department Responsibilities:**

- Notify and train the organization on the different data types (data dictionary)
- Provide the path for escalation (as listed above)

#### **5 Additional Resources**

##### **Contact for Support**

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

##### **Related Policies & Procedures**

Computer and Technology Use Policy  
Disaster Recovery Procedure  
Backup and Restoration Policy