July 2024

System Administration and Permissions 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

The technology department requires the highest level of admin access for all software systems to ensure efficient and effective management, maintenance, and security of critical technology infrastructure. This access level is essential for timely troubleshooting, configuration adjustments, and safeguarding against potential threats, enabling the department to fulfill its responsibilities in supporting the organization's operational and strategic objectives.

This policy establishes a standard for administration and permission assignments within all Water.org applications and systems. This policy defines the roles and responsibilities of the Technical Administrator and the Business Administrator.

Applicability

This policy applies to all enterprise digital solutions and/or software used within Water.org.

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

The technology department will work with the business administrator to establish the proper user account and permission level for the technical administrator account.

- The Technology department will maintain an administrative role/account defined at the highest level of access control. This is also often referred to as a Super User, Power User, or System Administrator.
- All enterprise digital systems will maintain a technical administrative account with access and administrative permission to all users, system, and security settings.
- Key business administrator account(s) will be created with similar access to use as needed.

2. Technical Administrator Account Permissions and Responsibilities

The list below defines the baseline of required permissions and responsibilities for the technology team administrator account. Every system is unique but in general the below list is the level of access needed:

2.1 Access

Manage advanced business level accounts (e.g., turnover)

2.2 Accessibility

Enabling and maintaining Single Sign On, multi-factor authentication, and/or other user access protocols

2.3 Managing Software Updates and Patches

This includes ensuring that all systems are up to date with the latest updates and patches to maintain security and performance. The process involves:

- Identifying and prioritizing updates and patches based on their importance and impact
- Testing updates and patches in a controlled environment before deploying them to production systems
- Deploying updates and patches to all relevant systems and monitoring their impact
- Documenting the updates and patches applied to maintain a record for future reference

2.4 System Design and Configuration

This includes support for: API access, integration configuration and support, scripting, data architecture

2.5 Optimization

The technical administrator should assist when systems performance issues arise and work with the business administrator to make necessary adjustments to optimize its efficiency. This might involve identifying and resolving bottlenecks or scalability issues.

2.6 System Security

Ensuring the security of the system is essential. This involves implementing and maintaining security measures to protect sensitive data and prevent unauthorized access.

2.7 Vendor/Account Management

The technical administrator will manage vendor contracts, renewals, and bill payment coordination for software systems.

3. Business Administrator Account Permissions and Responsibilities

It's the Technology department's expectation that a Business Lead or SME administrator has in-depth knowledge of the system they are responsible for. This includes understanding its functionality, configuration, and how it fits into the organization's overall technology infrastructure.

The list below defines the baseline of required permissions and responsibilities for the business lead administrator account. These expectations may vary depending on the complexity of the systems involved. Nonetheless, the role of a business administrator is critical for ensuring that systems are effectively managed, meet business needs, and contribute to the organization's success.

3.1 Business Logic Configuration or Settings

Defining, customizing, or setting up the specific operational guidelines, procedures, or regulations that govern the day-to-day functioning of a system, process, or organization.

3.2 Day to Day Responsibilities

The business administrator will be responsible for the day-to-day administration of the system. This includes tasks such as user account management, access control, system updates, and troubleshooting issues as they arise.

3.3 Training and Support

Responsible for training users on how to effectively use the system. This includes providing support, answering questions, and resolving issues to ensure that the system is being used efficiently:

- Standard User Account Management: Defining the roles, groups or permission levels (e.g., Profiles, etc.) for users and granting and removing user access when onboarding and offboarded.
- Communications: Effective communication is essential. Business administrators should be able to communicate technical information to non-technical stakeholders and work as a bridge between technical teams and business users.
- Import / Export of Data

3.4 Documentation

Maintaining up-to-date documentation is crucial. The business administrators should document system configurations, user guides, and any changes made to the system for reference and future troubleshooting.

3.5 Monitoring and Performance

Ensuring that applicable systems are configured for optimal performance, stability, and reliability. Work with technical administrator to resolve performance issues.

3.6 Compliance and Regulations

Depending on the industry, there may be regulatory requirements that the system must adhere to. The business administrators need to ensure that the system complies with relevant laws and regulations.

3.7 Continuous Improvement

Strive for continuous improvement by staying up to date with the latest developments in the field and identifying opportunities to enhance the system's functionality and performance.

III. Approval and Responsibility

Each department is responsible for managing and administering the daily tasks of the system.

The Technology Department has the approval and responsibility to administer all approved systems for the purpose of security, permissions, system integrations, etc.

IV. Additional Resources

Contact for Support

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

Related Policies

Security Handling Policy & Procedure

Identity Security Policy