Role-Based Access Control (RBAC) Access Management Policy and Procedure

1. Purpose

The purpose of this document is to establish a standard for role-based access control (RBAC) within our organization to ensure that employees have appropriate access to resources needed to perform their duties while protecting the security and confidentiality of information.

2. Scope

This policy applies to all employees, contractors, and third-party users of the organization who have access to the organization's information systems and resources.

3. Policy

3.1 General Principles

- Access to information resources is based on the principle of least privilege, ensuring individuals have access to only those resources necessary for their job functions.
- Roles are assigned based on job duties and responsibilities, and access rights are granted to roles rather than individuals.
- Periodic reviews of user access rights and roles are conducted to ensure compliance with this policy.

3.2 Role Definition

Roles are defined based on job functions and the access needs associated with those functions. Examples of roles include:

- **Administrator**: Full access to all systems and resources.
- **Manager**: Access to resources necessary for management tasks, such as reporting and employee oversight.
- **Employee**: Standard access to resources necessary for individual job functions.
- **IT Support**: Access to IT resources necessary for troubleshooting and support tasks.

3.3 Access Rights

Access rights for each role should be clearly defined and documented. These rights include:

- **Read**: View information and data.
- **Write**: Create or modify information and data.
- **Delete**: Remove information and data.
- **Execute**: Run specific processes or actions.

3.4 Access Management Procedure

1. **Request for Access**: Employees or their managers request access by submitting a formal access request form that specifies the necessary roles and justifies the need for access.
2. **Approval Process**: Access requests are reviewed by the department head or a designated authority who can approve or deny the request based on the alignment with job functions and the principle of least privilege.
3. **Implementation**: Upon approval, the IT department assigns the specified roles to the user, granting them the appropriate access rights.
4. **Review and Audit**: Regular audits are conducted to ensure access rights are in alignment with job responsibilities, and adjustments are made as necessary.

4. Enforcement

Violations of the RBAC policy will be met with disciplinary actions, which may include termination of employment, legal action, and restitution. The organization reserves the right to modify or revoke access rights at any time to ensure the security of its resources.

5. Review and Revision

This policy is reviewed annually or as required by changes in legislation, technology, or organizational needs. Revisions will be made as necessary to maintain the security and integrity of the organization's resources.