User Access Review Policy Template

Company Information

Company Name: [Insert Company Name]
Policy Contact: [Insert Contact Name or Department]
Effective Date: [Insert Date]
Review Date: [Insert Date]
Version: [Insert Version Number]

Company Overview

Provide a brief description of your company, including the nature of your business and any specific industry considerations that might impact the application of this policy.

Purpose

This policy establishes procedures and guidelines for conducting periodic reviews of user access rights across the organization's systems and applications. The purpose is to ensure that access privileges are appropriate, comply with the principle of least privilege, and support operational and security requirements.

Scope

This policy applies to all employees, contractors, consultants, and any other workers who have access to company information systems. The policy covers all systems, applications, and data to which access is controlled or regulated.

---

1. Definitions

- **User Access Review (UAR)**: The process of verifying and validating user access rights to systems and data.
- **Least Privilege**: The security principle that individuals should be granted the minimum level of access necessary to perform their job functions.
- **Privileged Access**: Access rights that allow users to perform administrative or specialized duties on IT systems.

---

2. Policy Statement

This policy mandates regular reviews of user access rights to ensure they remain appropriate and secure. The reviews will identify any discrepancies or excess privileges that need adjustment to maintain security and compliance with company policies.

---

3. Responsibilities

- **IT Security Team**: Lead and coordinate the User Access Review process, including preparation, execution, and follow-up actions.
- **Department Managers**: Review and validate access rights for their respective teams, ensuring accuracy and appropriateness.
- **Human Resources**: Provide current employment status information and communicate any changes such as terminations or role changes that might affect access rights.
- **Compliance Team**: Ensure that the UAR process meets regulatory requirements and company policies.

---

4. User Access Review Process

4.1 Scheduling and Planning

- User Access Reviews must be conducted at least bi-annually or more frequently based on the sensitivity of the information.
- The IT Security Team will schedule reviews and notify all stakeholders in advance.

4.2 Review Execution

- **System and Application List**: Compile a comprehensive list of all systems and applications subject to review.
- **User Access Report**: Generate current access rights reports from all systems and applications.
- **Review and Validation**:
    - Department Managers review access rights for appropriateness based on current job functions and responsibilities.
    - IT Security reviews for compliance with least privilege and security best practices.
    - Human Resources verifies employment status and role information.

4.3 Issues Identification

- Document any unauthorized, outdated, or excessive access rights found during the review.
- Highlight any discrepancies between recorded and actual access levels.

4.4 Remediation Actions

- Remove or adjust access rights that are not justified during the review process.
- Update records to reflect changes made during the review.

4.5 Documentation and Reporting

- Maintain detailed records of the review process, including changes made, persons involved in the review, and any issues identified.
- Prepare a summary report of the review outcomes for management and audit purposes.

---

5. Exception Handling

- Any deviations from standard access rights must be documented and approved by the relevant department manager and the IT Security Team.
- Exceptions must be reviewed during each User Access Review cycle to ensure they are still valid.

---

6. Training and Awareness

- Provide regular training to all employees and stakeholders involved in the User Access Review process.
- Raise awareness about the importance of security and compliance in managing access rights.

---

7. Monitoring and Enforcement

- The IT Security Team will monitor compliance with this policy and conduct random audits to ensure the integrity of the User Access Review process.
- Non-compliance with this policy may result in disciplinary actions, up to and including termination of employment.

---

8. Policy Review

- This policy will be reviewed annually or following significant changes to business processes or IT infrastructure.
- Revisions will be made to address new security challenges and regulatory requirements.

Approval
This policy has been reviewed and approved by the organization's executive team.

Signature of Executive Officer: _____

Name: [Executive Name]

Title: [Executive Title]

Date of Approval: [Approval Date]
