IJEZIE
RISK ADVISORY

ACCESS CONTROL & PRIVILEDGED ACCESS POLICY

Governing User and Privileged Access to Protect Organizational Systems and Data

Ifeanyi Ijezie

Ijezie Risk Advisory | https://github.com/ijeziermf

Access Control & Privileged Access Policy

Version: 1.0

Effective Date: _______________

Policy Owner: Information Security

Review Frequency: Annual

1. Purpose

The purpose of this policy is to establish requirements for managing access to organizational systems, applications, and data in order to reduce the risk of unauthorized access, misuse of privileges, and security incidents. This policy ensures that access is granted based on business need and limited to the minimum level required to perform authorized job functions.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and third parties who access organizational systems or data. It covers all information systems, applications, networks, and data assets owned, managed, or processed on behalf of the organization, including on-premises, cloud, and third-party hosted environments.

3. Policy Statements

3.1 Access Control Principles

- Access to systems and data shall be granted based on the principle of least privilege.
- Users shall be provided only the access necessary to perform their assigned job responsibilities.
- Access rights shall be approved by an authorized system or data owner prior to provisioning.
- Access shall be granted based on documented business justification.

3.2 Privileged Access Management

- Privileged accounts shall be limited to personnel with a documented operational or administrative need.
- Privileged access shall be provisioned separately from standard user access.
- The use of shared or generic privileged accounts is prohibited unless explicitly approved and documented.
- Privileged account activity shall be logged and subject to monitoring.
- Privileged access shall be time-bound where feasible and revoked when no longer required.

3.3 Access Provisioning and Deprovisioning

- Access shall be provisioned following identity verification and formal approval.
- Access shall be reviewed and updated promptly upon role change, job transfer, or change in responsibilities.
- All access shall be revoked immediately upon termination of employment or contract, in accordance with offboarding procedures.
- Temporary access shall be removed upon completion of the approved activity or expiration of the approval period.

3.4 Access Reviews

- Periodic access reviews shall be conducted to confirm that user access remains appropriate.
- Privileged access shall be reviewed at least quarterly or more frequently based on risk.
- Identified access discrepancies shall be remediated in a timely manner.
- Evidence of access reviews and remediation actions shall be retained in accordance with organizational record-keeping requirements.

3.5 Authentication Requirements

- Multi-factor authentication shall be enforced for privileged access where technically feasible.
- Authentication credentials shall not be shared between users.
- Default credentials shall be changed prior to system use.
- Strong authentication mechanisms shall be used in accordance with organizational standards.

4. Roles and Responsibilities

Information Security

- Defines access control requirements, provides guidance, monitors compliance, and supports enforcement of this policy.

System and Data Owners

- Approve access requests, participate in access reviews, and ensure access aligns with business requirements.

Managers

- Ensure access reflects job responsibilities and initiate access changes when personnel roles change.

Users

- Use access responsibly and report suspected unauthorized access or credential compromise.

5. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. Violations may also result in legal, regulatory, or contractual consequences. All suspected violations shall be investigated in accordance with organizational procedures.

6. Review and Maintenance

This policy shall be reviewed at least annually or upon significant changes to organizational systems, roles, or regulatory requirements. Updates shall be approved by appropriate governance authorities and communicated to relevant stakeholders.

7. Framework Alignment Reference

- NIST Cybersecurity Framework: PR.AC
- NIST SP 800-53: AC (Access Control), IA (Identification and Authentication)
- ISO/IEC 27001: Access Control (Annex A)

This policy is intended to support organizational governance and cyber risk management and may be adapted to align with specific operational, regulatory, or business requirements.

Document Control

Document ID	IRA-AC-001
Approved By	____________________________
Classification	Internal
Next Review Date	____________________________