IJEZIE
RISK ADVISORY

SECURITY AWARENESS & ACCEPTABLE USE POLICY

Governance Requirements for Responsible and Secure Use of Organizational Systems

Ifeanyi Ijezie

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

Security Awareness & Acceptable Use Policy

Version: 1.0

Effective Date: _____

Policy Owner: Information Security

Review Frequency: Annual

1. Purpose

The purpose of this policy is to define acceptable use requirements and security awareness expectations for individuals who access organizational systems, applications, or data. This policy is intended to reduce cyber risk by promoting responsible system use, strengthening user awareness of security threats, and establishing clear expectations for protecting organizational information assets.

2. Scope

This policy applies to all employees, contractors, consultants, temporary workers, and third parties who access organizational systems, networks, applications, or data. It applies to all organizational computing resources, including on-premises systems, cloud services, mobile devices, and third-party hosted environments.

3. Policy Statements

3.1 Security Awareness and Training

- All users shall complete security awareness training upon onboarding and at least annually thereafter.
- Security awareness training shall address common cyber threats, including phishing, social engineering, credential misuse, and data protection responsibilities.
- Role-based or enhanced training may be required for users with privileged access or elevated risk exposure.
- Completion of required training shall be tracked and monitored by Information Security.

3.2 Acceptable Use of Systems

- Organizational systems and data shall be used for authorized business purposes only.
- Users shall not engage in activities that could compromise the confidentiality, integrity, or availability of systems or data.
- Unauthorized software installation, system modification, or circumvention of security controls is prohibited.
- Users shall comply with all applicable organizational policies, standards, and procedures when using organizational resources.

3.3 Credential and Account Responsibilities

- Users are responsible for safeguarding authentication credentials and shall not share credentials with others.
- Strong passwords or authentication mechanisms shall be used in accordance with organizational requirements.
- Users shall promptly report suspected credential compromise or unauthorized access.
- Default or temporary credentials shall be changed upon initial use.

3.4 Data Handling and Protection

- Organizational data shall be handled in accordance with applicable data classification and protection requirements.
- Sensitive or confidential data shall not be stored, transmitted, or shared using unauthorized methods.
- Users shall exercise caution when accessing organizational data from remote or public locations.
- Loss or unauthorized disclosure of organizational data shall be reported immediately.

3.5 Prohibited Activities

- Users shall not use organizational systems for illegal, unethical, or unauthorized activities.
- Use of organizational resources to access, distribute, or store inappropriate or malicious content is prohibited.
- Attempts to bypass security controls, monitoring, or logging mechanisms are prohibited.
- Use of organizational systems in a manner that disrupts operations or degrades system performance is prohibited.

3.6 Reporting Security Concerns

- Users shall promptly report suspected security incidents, phishing attempts, or policy violations.
- Reporting shall occur through designated channels without fear of retaliation.
- Early reporting supports timely response and risk reduction.

4. Roles and Responsibilities

Information Security

- Develops security awareness content, monitors compliance, and provides guidance on acceptable use requirements.

Managers

- Ensure personnel complete required training and adhere to acceptable use expectations.

Users

- Comply with this policy, complete required training, and report suspected security issues promptly.

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, threat landscape, or regulatory requirements. Updates shall be approved by appropriate governance authorities and communicated to relevant stakeholders.

7. Framework Alignment Reference

- NIST Cybersecurity Framework: PR.AT
- NIST SP 800-53: AT (Awareness and Training), PL (Planning)
- ISO/IEC 27001: Human Resource Security and Acceptable Use (Annex A)

This policy is intended to support organizational security awareness, responsible system use, and cyber risk reduction and may be adapted to align with specific operational, regulatory, or business requirements.

Document Control

Document ID	IRA-AT-001
Approved By	_____
Classification	Internal
Next Review Date	_____