US Solutions Pvt Ltd. - Access Control Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-01-05
- **Author:** IT & Infosec Department - Kevin Nguyen
- **Approved By:** Patricia Rodriguez, Head of Security Operations
- **Effective Date:** 2024-02-01
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that robust access control mechanisms are essential for protecting the confidentiality, integrity, and availability of our information assets. This Access Control Policy outlines the principles and procedures for granting, managing, and revoking access to Company systems, applications, and data. All employees, contractors, and authorized users ("Users") are required to adhere to this policy to ensure the security of our information resources.

2. Purpose

The purpose of this policy is to:

- Establish a standardized approach to access control.
- Ensure that access is granted on a need-to-know and least-privilege basis.
- Protect sensitive information from unauthorized access and disclosure.
- Facilitate compliance with applicable laws and regulations.
- Define the responsibilities of access requestors, approvers, and administrators.

3. Scope

This policy applies to all Users who access Company systems, applications, and data, including but not limited to:

- Network accounts and servers.
- Company applications (e.g., CRM, ERP).
- Databases and file shares.
- Cloud-based services.
- Physical access to Company facilities.
- Remote access to Company resources.

4. Principles of Access Control

- **Least Privilege:** Users should be granted only the minimum level of access necessary to perform their job functions.
- **Need-to-Know:** Access to sensitive information should be granted only to those who have a legitimate business need.
- **Separation of Duties:** Responsibilities should be divided among multiple individuals to prevent fraud and errors.

- **Regular Reviews:** Access rights should be reviewed periodically to ensure they remain appropriate.
- **Auditing:** Access logs should be maintained and regularly audited to detect unauthorized access.

5. Access Request and Approval Process

- **Access Request:** Users must submit a formal access request through the Company's designated system or process.
- **Approval:** Access requests must be approved by the User's manager and, if applicable, the data owner or system administrator.
- **Documentation:** All access requests and approvals must be documented and retained for audit purposes.
- **Temporary Access:** Temporary access can be granted for specific projects or tasks, with a defined expiration date.

6. User Account Management

- **Account Creation:** User accounts should be created only after receiving proper authorization.
- **Account Naming Conventions:** User accounts must adhere to the Company's standardized naming conventions.
- **Password Management:** User passwords must comply with the Company's Password Policy.
- **Account Termination:** User accounts must be disabled or deleted immediately upon termination of employment or contract.

7. Access Control Mechanisms

- **Role-Based Access Control (RBAC):** Access rights should be assigned based on user roles and responsibilities.
- **Attribute-Based Access Control (ABAC):** Access rights can be granted based on user attributes, resource attributes, and environmental conditions.
- **Multi-Factor Authentication (MFA):** MFA is mandatory for access to sensitive systems and applications.
- **Physical Access Control:** Physical access to Company facilities must be controlled through access cards, keypads, or other security measures.
- **Remote Access Control:** Remote access to Company resources must be secured through VPNs and MFA.

8. Access Reviews and Audits

- **Periodic Reviews:** Access rights should be reviewed at least annually to ensure they remain appropriate.
- **Audit Logs:** Access logs should be maintained and regularly audited to detect unauthorized access.
- **Incident Response:** Any suspected security incidents related to access control must be reported immediately to the IT department.

9. Responsibilities

- **Users:**
  - Request access through the designated process.
  - Protect their access credentials.
  - Report any unauthorized access attempts.
  - Comply with this policy.
- **Managers:**
  - Approve access requests for their team members.
  - Ensure that access rights are appropriate for job functions.
  - Report any security concerns to the IT department.
- **IT Department:**
  - Implement and maintain access control systems.
  - Manage user accounts and access rights.
  - Conduct regular access reviews and audits.
  - Investigate and respond to security incidents.
- **Data Owners:**
  - Determine access requirements for their data.
  - Approve access requests for their data.
  - Review access rights periodically.

10. Legal and Regulatory Compliance

- This policy complies with all applicable data privacy laws and regulations (e.g., GDPR, CCPA).
- Access control measures must be consistent with legal and regulatory requirements.

11. Training and Awareness

- All Users will receive training on this Access Control Policy.
- Regular security awareness training will be provided to reinforce access control best practices.

12. Policy Review and Updates

- This policy will be reviewed and updated annually or as needed to reflect changes in technology, threats, and regulations.
- Any updates to this policy will be communicated to all Users.

13. Acknowledgement

- By accessing Company systems, applications, and data, Users acknowledge that they have read, understood, and agree to comply with this Access Control Policy.

This Access Control Policy is designed to protect US Solutions Pvt Ltd.'s information assets and ensure compliance with applicable laws and regulations. By adhering to these guidelines, Users contribute to a secure and compliant work environment.