US Solutions Pvt Ltd. - User Provisioning and Deprovisioning Policy

Document Control:

- **Version:** 1.0
- **Date Issued:** 2024-03-22
- **Author:** IT & Infosec Department - Leonardo Sanchez
- **Approved By:** Victoria Grant, Systems Administration Manager
- **Effective Date:** 2024-04-22
- **Review Frequency:** Annually

1. Introduction

US Solutions Pvt Ltd. recognizes that effective user provisioning and deprovisioning are crucial for maintaining system security and ensuring appropriate access to company resources. This policy outlines the procedures for creating, modifying, and terminating user accounts and access rights. All employees, contractors, and authorized users ("Users") are required to adhere to this policy.

2. Purpose

The purpose of this policy is to:

- Establish a standardized process for user account management.
- Ensure that access is granted on a need-to-know and least privilege basis.
- Prevent unauthorized access to company systems and data.
- Maintain accurate user account information.
- Facilitate compliance with applicable laws, regulations, and industry standards.

3. Scope

This policy applies to all user accounts that access company systems, applications, and data, including:

- Network accounts and servers.
- Email and messaging systems.
- Company applications (e.g., CRM, ERP).
- Databases and file shares.
- Cloud-based services.
- Remote access systems.
- Physical access control systems.

4. User Provisioning Procedures

- **Account Request:**
    - A formal account request must be submitted by the User’s manager or HR department.

    - The request must include the User's name, job title, department, and required access rights.
    - The request must be approved by the appropriate authority (e.g., department head, system owner).
- **Account Creation:**
    - User accounts will be created by the IT department according to company naming conventions.
    - Access rights will be assigned based on the User's job role and responsibilities.
    - Temporary accounts may be created for contractors or temporary staff, with a defined expiration date.
- **Account Information:**
    - User account information must be accurate and up-to-date.
    - Users are responsible for maintaining their contact information.
    - The IT department will verify account information periodically.
- **Access Review:**
    - Access rights will be reviewed periodically to ensure they remain appropriate.
    - User access will be reviewed upon job changes or department transfers.
    - Access reviews will be documented and retained for audit purposes.

5. User Deprovisioning Procedures

- **Account Termination:**
    - User accounts must be disabled immediately upon termination of employment or contract.
    - The HR department is responsible for notifying the IT department of account terminations.
    - Access to physical access systems must also be revoked.
- **Data Transfer:**
    - Upon termination, the User's data must be transferred or backed up according to company policy.
    - The User's manager is responsible for ensuring that necessary data is transferred.
- **Account Deletion:**
    - User accounts and associated data must be deleted according to company data retention policies.
    - Audit logs must be retained for a defined period.
    - Email accounts must be archived and then deleted.
- **Access Revocation:**
    - All access rights must be revoked upon termination or job change.
    - Access to physical access systems must also be revoked.
    - Remote access privileges must be terminated.

6. Responsibilities

- **Human Resources (HR):**
    - Notify the IT department of new hires and terminations.
    - Provide accurate employee information.

- **Managers:**
    - Submit account requests and approvals.
    - Ensure that access rights are appropriate for job functions.
    - Inform IT of employee role changes.
    - Ensure data transfer upon termination.
- **IT Department:**
    - Create, modify, and terminate user accounts.
    - Manage access rights and permissions.
    - Maintain accurate user account information.
    - Conduct access reviews and audits.
    - Maintain logs of all changes.
- **Users:**
    - Comply with this policy.
    - Protect their access credentials.
    - Report any unauthorized access attempts.
    - Ensure personal contact information is up to date.

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.
- **Privileged Access Management (PAM):** PAM solutions must be used to manage privileged accounts.

8. Legal and Regulatory Compliance

- This policy complies with all applicable data privacy laws and regulations (e.g., GDPR, CCPA).
- User provisioning and deprovisioning practices must be consistent with legal and regulatory requirements.

9. Training and Awareness

- All Users involved in user account management will receive training on this policy.
- Regular security awareness training will be provided to reinforce access control best practices.

10. 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.

11. Monitoring and Enforcement

- The IT department will conduct regular audits to ensure compliance with this policy.
- Violations of this policy may result in disciplinary action, up to and including termination of employment or contract.

12. Acknowledgement

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

This User Provisioning and Deprovisioning 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.