Standard Operating Procedure (SOP): IT and Systems Access Provisioning

This SOP details the process for **IT and systems access provisioning**, including user account creation, role-based access assignment, password and authentication management, access approval workflows, periodic access reviews, and de-provisioning procedures. The goal is to ensure secure and efficient access control to IT systems and resources, protecting organizational data and maintaining compliance with security policies.

1. Purpose

To define a standardized process for granting, modifying, reviewing, and revoking access to organizational IT systems and applications, ensuring only authorized users have appropriate access according to their roles and responsibilities.

2. Scope

This SOP applies to all employees, contractors, and third-party users who require access to the organization's IT systems and applications.

3. Responsibilities

- **HR Department:** Notifies IT of new hires, role changes, and terminations.
- **IT Department:** Manages provisioning, modifications, and de-provisioning of access.
- **System/Resource Owners:** Approve access requests for their systems or datasets.
- **Managers/Supervisors:** Initiate access requests and approve or reject user access changes.
- **Users:** Use access only as authorized; report any access issues or security incidents.

4. Definitions

Term	Definition
Provisioning	The process of creating and granting access to IT systems for users.
De-provisioning	Removing or disabling access for users who no longer require it.
Role-Based Access Control (RBAC)	Assigning system access based on user roles within the organization.

5. Procedure

5.1. User Account Creation

1. HR notifies IT of a new hire, supplying required personal and role information.
2. IT creates the user's account(s) in necessary IT systems, following RBAC principles.
3. Default access is limited to the minimum required for the user's role.

5.2. Role-Based Access Assignment

1. Access to applications and resources is granted based on the user's job function, verified against approved role templates.
2. Any exception or additional access beyond role-based templates requires written justification and approval.

5.3. Password and Authentication Management

1. Initial passwords are system-generated and must be changed upon first login.
2. Enforce strong password policies (e.g., minimum length, complexity requirements).
3. Enable multi-factor authentication (MFA) wherever feasible.

5.4. Access Approval Workflow

1. All access requests must be logged in the ticketing system or access management portal.
2. Requests are reviewed and approved/rejected by the designated manager and resource owner.
3. IT provisions access only after receipt of all required approvals.

5.5. Periodic Access Reviews

1. Conduct access reviews at least quarterly, or as required by regulatory policies.
2. Managers and system owners must validate user access and request removal or changes as appropriate.
3. Document and resolve any discrepancies identified during reviews.

5.6. De-Provisioning Procedures

1. HR notifies IT promptly of employee terminations or role changes.
2. IT disables/removes user access on or before the effective date of separation or role change.
3. Recover or transfer any organizational data or assets held by the user.
4. Document de-provisioning actions in the access management system.

6. Supporting Documentation

- User Access Request Form
- Access Review Checklist
- De-provisioning Log Template
- IT Security Policy

7. Compliance and Audit

All access provisioning and de-provisioning activities are subject to internal audits and must comply with the organization's security policies and relevant regulations (e.g., GDPR, HIPAA, SOX).

8. Revision History

Version	Date	Description	Author
1.0	2024-06-12	Initial template creation	IT Security Team