Access and Identity Management SOP

This SOP establishes **access and identity management** protocols to ensure secure and efficient control of user identities and access rights within an organization. It covers user authentication and authorization processes, account provisioning and de-provisioning, password and credential management, role-based access controls, audit and monitoring procedures, and compliance with security policies and regulatory requirements. The goal is to protect sensitive information and systems by managing user access in a standardized and controlled manner.

1. Purpose

To define standardized processes for managing user identities and controlling access to organizational information systems and resources.

2. Scope

This SOP applies to all employees, contractors, temporary staff, and third-party vendors with access to organizational systems and networks.

3. Responsibilities

Role	Responsibility
IT Security Team	Oversee access management processes, maintain IAM tools, monitor compliance.
Managers	Approve access requests, validate access levels, notify IT of role changes.
HR Department	Notify IT of new hires, terminations, or changes in employment status.
End Users	Comply with access policies, report suspicious activity, maintain password confidentiality.

4. Procedures

4.1 User Account Provisioning

- New user request initiated by hiring manager/HR.
- Appropriate access roles determined based on job responsibilities.
- IT provisions user account according to approved roles.
- Default credentials sent securely to user for initial login.

4.2 User Account De-Provisioning

- Upon termination or role change, HR notifies IT Security Team.
- IT immediately disables or adjusts access accordingly.
- Accounts are reviewed and deactivated or deleted within 24 hours of notice.

4.3 Access Authorization

- Access requests submitted via standardized form or ticketing system.
- Managerial approval required for access above baseline roles.
- IT grants access and updates access logs.

4.4 Password and Credential Management

- Passwords must meet complexity requirements (length, characters, etc.).
- Passwords to be changed every 90 days; reuse restricted.
- Multi-factor authentication (MFA) required for privileged accounts.
- Credential storage compliant with organizational security standards.

4.5 Role-Based Access Control (RBAC)

- Access rights granted based on job roles and responsibilities.
- Roles reviewed and updated as needed, at least annually.

4.6 Audit and Monitoring

- Regular audits conducted to ensure correct access assignments.
- System access logs reviewed for unusual or unauthorized activity.
- Audit findings documented and addressed in a timely manner.

4.7 Compliance and Review

- Access management processes aligned with legal, regulatory, and organizational requirements.
- SOP reviewed annually or after significant process changes.

5. Documentation

- Access request/approval forms
- User access review logs
- Incident reports
- Audit reports

6. Enforcement

Violations of this SOP may result in disciplinary action up to and including termination, as well as potential legal action in accordance with organizational policies.

7. Review and Revision

This SOP will be reviewed at least annually or in response to significant changes in technology, policy, or regulatory requirements.