STANDARD OPERATING PROCEDURE

Access Management Procedure

Financial Services Entity
Information Technology Department

Version 1.0
9 January 2026

Prepared by: Hasan Raza

CONFIDENTIAL - Internal Use Only

DOCUMENT CONTROL

Department	**[IT Operations]**
Version	1.0
Status	Final
Owner	IT Manager – Access Management
Author	Hasan Raza
Last Review Date	01/9/2026
Next Review Date	12/9/2026

APPROVALS

Role	Name	Date
IT Manager	Isaac Peshach	01/9/2026
CISO/Security Lead	Dre Medici	01/9/2026
Compliance Officer	Gabriela Noboa	01/9/2026

1. Purpose

This procedure defines the standardized process for managing user access throughout its lifecycle (provisioning, modification, review, and de-provisioning). The objective is to reduce the risk of unauthorized access, data breaches, and regulatory non-compliance.

2. Scope

This procedure applies to all employees, contractors, and third parties with access to corporate systems, including cloud platforms, internal applications, databases, and administrative interfaces.

3. Authority & Compliance Alignment

This procedure is authorized under the Information Security Policy and supports compliance with:

- ISO/IEC 27001:2022 (Annex A – Access Control)
- NIST SP 800-53 (AC-2, AC-6)
- SOC 2 (CC6 – Logical Access Controls)
- SBP Cybersecurity Framework

4. Procedures

Step 1: User Access Provisioning

Trigger: HR onboarding request
Responsible Role: IT Administrator Actions:
1. Validate user role and manager approval.
2. Create user account following least-privilege principles.
3. Enforce MFA for all privileged and remote access.
Validation: Manager approval recorded.
Evidence: HR ticket, IAM logs.

Step 2: Access Review

Trigger: Monthly scheduled review
Responsible Role: IT Manager Actions:
1. Review active user access list.
2. Remove excessive or unused privileges.
Validation: Signed access review report.
Evidence: Access review records.

Step 3: De-Provisioning

Trigger: Employee off-boarding notification
Responsible Role: IT Administrator Actions:
1. Disable all system access within 24 hours.
2. Revoke VPN, cloud, and admin access.
Validation: Account status shows disabled.
Evidence: IAM audit logs.

5. CONTROL MAPPING

This procedure implements the following security controls:

Framework	Control ID	SOP Section	Evidence of Implementation
NIST 800-53	AC-2(Account Management), AC-6(Least Privilege)	Step 1 – User Access Provisioning Step 2 – Access Review	HR onboarding tickets, IAM approval logs, Access review reports
ISO 27001	A.5.15(Access Control), A.5.18(Access Rights)	Step 1 – User Access Provisioning Step 3 – DeProvisioning	Active Directory logs, Okta/IAM audit trails, Off-boarding records
SOC 2	CC6.1(Logical Access Security)	Step 2 – Access Review Step 3 – DeProvisioning	Access certification reports, GRC tool records, Change logs

6. RELEVANT LINKS

- **Information Security Policy**
- **Access Control Policy**
- **User Provisioning & De-Provisioning Guidelines**
- **Incident Response Plan**
- **Identity & Access Management (IAM) System Documentation**

7. REVISION HISTORY

Date	Version	Author	Summary of Changes
01/9/2026	1.0	Hasan Raza	Initial release