Standard Operating Procedure

SOP-IT-007: Access & Security Management

Document ID:	SOP-IT-007	**Version:**	1.0
Effective Date:	YYYY-MM-DD	**Review Date:**	YYYY-MM-DD

1. Purpose

This SOP defines access control, authentication, and security management for IT systems in compliance with 21 CFR Part 11.

2. Scope

This SOP applies to all systems requiring user authentication and access control, including GitHub, AWS, databases, and laboratory systems.

3. Access Control Principles

- **Least Privilege: Users get minimum access needed**
- **Role-Based Access Control (RBAC)**
- **Multi-Factor Authentication (MFA) required**
- **Access review every 90 days**

4. User Provisioning

New User:

- Submit access request via FORM-002
- Manager approval required
- Training completion verified (SOP-IT-006)
- Access granted by SRE Lead

User Departure:

- All access revoked within 24 hours
- GitHub keys, AWS credentials rotated

5. Security Requirements

- MFA enforced on all accounts
- Password policy: 12+ chars, complexity, 90-day rotation
- Session timeout: 30 minutes inactivity
- Audit logs retained 7+ years

6. Approvals

This document requires electronic signature approval via DocuSign (21 CFR Part 11 compliant).

Role	**Name**	**Signature & Date**
Author	[Name]	[DocuSign]
Reviewer (QA Lead)	[Name]	[DocuSign]
Approver (Quality Manager)	[Name]	[DocuSign]