



BrainSAIT Information Security Policy

■■■■■ ■■■■ ■■■■ - Information Security Policy

Document Type:	Company Policy
Department:	Technology
Version:	2.1
Date:	November 07, 2025
Author:	BrainSAIT
Classification:	INTERNAL USE - MANDATORY COMPLIANCE

CONFIDENTIAL - HIPAA PROTECTED
■■■ - ■■■■ ■■■■ HIPAA



Policy Information



Effective Date: November 07, 2025
Next Review Date: November 07, 2026
Policy Owner: Technology Department
Approved By: BrainSAIT Executive Committee
Compliance Framework: HIPAA, NPHIES, ISO 27001

1. Purpose and Scope

1.

Purpose: This policy establishes the standards and requirements for information security across all BrainSAIT operations, systems, and data assets. It ensures compliance with healthcare regulations and protects patient health information (PHI) and personally identifiable information (PII).

Scope: This policy applies to all BrainSAIT employees, contractors, partners, and third-party vendors who have access to company systems, data, or facilities. It covers all information assets regardless of form or location.

2. Policy Statements

2.

2.1 Data Classification: All data must be classified according to sensitivity levels: Public, Internal, Confidential, and Restricted (PHI/PII).

2.2 Access Control: Access to systems and data shall be granted based on the principle of least privilege and role-based access control (RBAC). All access requests must be approved by department managers and logged.

2.3 Encryption: All PHI and PII must be encrypted at rest using AES-256 and in transit using TLS 1.3. Encryption keys must be managed using approved key management systems.

2.4 Audit Logging: All system access, data modifications, and security events must be logged with comprehensive audit trails retained for minimum 7 years. Logs must be regularly reviewed for anomalies.

2.5 Incident Response: Security incidents must be reported within 1 hour of discovery. The incident response team will investigate and remediate according to established procedures.

3. Roles and Responsibilities

3. ■■■■■■■■ ■■■■■■■■■■

Executive Management: Approve policy, allocate resources, enforce compliance

Department Managers: Implement policy in departments, approve access requests

IT Security Team: Monitor compliance, conduct audits, manage security tools

All Employees: Comply with policy, report incidents, complete training

4. Compliance and Enforcement

4. ■■■■■■■■ ■■■■■■■■■■

Compliance Monitoring: Quarterly audits will be conducted to ensure policy compliance. Non-compliance will be documented and remediation plans required.

Training Requirements: All personnel must complete annual security awareness training. New hires must complete training within 30 days.

Violations: Policy violations may result in disciplinary action up to and including termination. Serious violations will be reported to regulatory authorities as required by law.

5. Related Documents

5. ■■■■■■■■ ■■■ ■■■■■■

- Acceptable Use Policy
- Data Protection Policy
- Incident Response Procedure
- Access Control Procedure
- HIPAA Compliance Manual
- Business Continuity Plan