ISO27001:2022

NimbusTech Solutions, Inc.

ISMS Policy Document

Version 1.0

August 2025

Table of Contents

1. Document Control

Field	Details
Document Title	Information Security Management System (ISMS) Policy
Document ID	NT-ISMS-POL-001
Version	1.0
Version History	Version 1.0 - 2025-08-15 - Initial Release - Author: Laura Chen (ISMS Manager) - Approved: Rajesh Patel (CISO)
Approval Date	2025-08-15
Review Date	2026-08-15
Approved By	Amelia Hartman, CEO
Owner	Rajesh Patel, CISO
Classification	Public
Distribution List	All Employees, Contractors, Approved Vendors
Storage Location	NimbusTech Intranet > Policies > ISMS

2. Purpose & Policy Objectives

a. Purpose :

This policy defines the framework for managing information security within NimbusTech Solutions, Inc., ensuring compliance with ISO/IEC 27001 requirements and protecting the confidentiality, integrity, and availability of information assets.

b. Policy Objective :

i. Provide strategic direction for information security initiatives.
ii. Support business continuity through proactive risk management.
iii. Ensure compliance with legal, regulatory, and contractual requirements.

3. Scope

a. In-Scope Assets :

i. Corporate network infrastructure
ii. Production cloud environments
iii. Company-owned endpoints and mobile devices
iv. Business applications and SaaS platforms

b. In-Scope Personnel :

All NimbusTech employees, contractors, and managed service providers with system or data access.

c. Physical Locations Covered :

i. Austin, TX Headquarters
ii. Data Center facilities in Dallas, TX
iii. Approved home offices of remote employees

d. Exclusions :

Personal devices not enrolled in Mobile Device Management (MDM)

4. Definitions & Acronyms

a. ISMS : Information Security Management System
b. CIA Triad : Confidentiality, Integrity, Availability
c. PII : Personally Identifiable Information
d. GDPR : General Data Protection Regulation
e. HIPAA : Health Insurance Portability and Accountability Act
f. SoA : Statement of Applicability
g. BCP : Business Continuity Plan

5. Policy Statement

NimbusTech Solutions is committed to safeguarding its information assets from unauthorized access, disclosure, alteration, or destruction. The organization will implement, maintain, and continually improve an ISMS that aligns with ISO/IEC 27001 to protect customer trust, meet compliance obligations, and support business objectives.

6. Guiding Principles

a. Confidentiality : Information will be accessible only to authorized parties.
Integrity : Information will remain accurate, complete, and unaltered.
Availability : Systems and data will be accessible to authorized users when required.

b. Risk-Based Approach : Security Controls will be selected and prioritized based on risk assessment results.
c. Legal and Regulatory Compliance : The organization will comply with all applicable laws and regulations.
d. Continual Improvement : Security processes will be regularly reviewed and enhanced.

7. Roles & Responsibilities

a. Board of Directors / Executive Management : Provide strategic direction and approve ISMS resources.
b. CISO : Lead ISMS development, implementation, and performance monitoring.
c. ISMS Manager : Maintain ISMS documentation and coordinate audits.
d. Department Heads : Ensure departmental compliance with ISMS requirements.
e. All Employees : Adhere to security policies and report incidents.
f. External Vendors / Third Parties : Comply with contractual security requirements and the Vendor Management Policy.

8. Information Security Objectives

a. Maintain uptime of critical services at 99.9% or higher.
b. Achieve zero high-severity security incidents annually.
c. Ensure 100% completion rate of annual security awareness training by employees.
d. Conduct risk assessments at least once annually.

9. Risk Management Commitment

a. Approach to Risk Identification & Assessment

NimbusTech will establish and maintain a systematic process for identifying, analyzing, and evaluating information security risks. Risk assessments will be conducted:

- At least annually.
- When significant changes occur in the organization's structure, technology, or processes.
- Following major security incidents.

Risks will be assessed using defined criteria for likelihood and impact, and the results will guide the selection of appropriate risk treatment measures in alignment with ISO/IEC 27005 and Annex A of ISO/IEC 27001.

b. Link to Risk Methodology Document

10. ISMS Governance Framework

a. Governance Structure for ISMS

The ISMS will be governed under the direction of the CISO and the ISMS Manager.

b. Key ISMS documents

i. Statement of Applicability (SoA)
ii. Risk Methodology Document
iii. Risk Register
iv. Incident Response Policy
v. Business Continuity Plan

11. Compliance & Legal Requirements

a. Applicable Laws and Regulations

NimbusTech will identify, monitor, and comply with all relevant legal and regulatory requirements that impact the confidentiality, integrity and availability of its information assets, including but not limited to:

- General Data Protection Regulation (GDPR) - applicable to processing of EU personal data.
- Health Insurance Portability and Accountability Act (HIPAA) - applicable to certain U.S. Healthcare client data.
- U.S. State Data Breach Notification Laws - applicable to incidents involving personal data of state residents.
- Any other applicable national or international data protection, privacy, and cybersecurity regulations.

b. Contractual Obligations

NimbusTech will meet all information security requirements set forth in:

- Client contracts and service agreements.
- Non-Disclosure Agreements (NDAs).
- Vendor and supplier contracts containing security clauses.
- Industry-specific security standards mandated through agreements - NIST 800-171 for government clients.

c. Certification Commitments

NimbusTech is committed to achieving, maintaining and improving recognized industry certifications to demonstrate its information security capabilities, including but not limited to:

- ISO/IEC 27001 certification for its Information Security Management System.
- SOC 2 Type II compliance for service reliability and trust.
- Any additional certifications as required by business strategy or client requirements.

Compliance with all laws, contractual requirements, and certification obligations reviewed during ISMS management will be reviewed and verified through Internal and external audits.

12. Asset Classification & Handling

a. Overview

- Assets will be classified into four categories : Public, Internal, Confidential, Restricted.
- Classification determines handling, storage, and transmission requirements.

b. Reference: Asset Classification & Handling Policy

13. Awareness & Training

- All employees must complete security awareness training annually.
- New hires must complete training within 30 days of joining.
- Repeated policy violations may result in disciplinary action, up to and including termination.

14. Continual Improvement

- The ISMS will be reviewed at least annually through management reviews and internal audits.
- Lessons learned from incidents will be integrated into policy updates.

15. Communication

- This policy will be published on the company intranet.
- Customers and stakeholders may request a copy of the public ISMS Policy.

- Employees can report incidents via the IT Helpdesk or Security Hotline.

16. Policy Review & Approval

a. Review Frequency:

Annually or upon significant changes in operations, technology, or legal requirements.

b. Approval Record:

Approved by: Amelia Hartman, CEO
Date: 2025-08-15