NimbusTech Solutions, Inc.

Statement of Applicability (SoA)

Document ID: NT-ISMS-SoA-001
Version: 1.0
Date: August 15, 2025
Owner: Rajesh Patel, CISO
Approved By: Amelia Hartman, CEO

Purpose

This Statement of Applicability (SoA) identifies which of the ISO/IEC 27001:2022 Annex A controls are applicable to NimbusTech's ISMS, the justification for their inclusion or exclusion, and their current implementation status. The SoA forms the link between the Risk Register, Risk Treatment Plan, and the organization's ISMS framework.

SoA Matrix:

(Sample Portfolio Version - 18 Controls)

Control No.	Control Name	Applicable	Justification	Implementation Status	Reference Document
A.5.1	Policies for Information Security	Yes	Core requirements for ISMS governance and overall direction.	Implemented	ISMS Policy
A.5.2	Information Security Roles & Responsibilities	Yes	Required for accountability and clarity in the ISMS framework.	Implemented	ISMS Policy, Job Descriptions
A.5.5	Contact with Authorities	Yes	Needed for incident escalation and compliance with regulatory reporting.	Partially Implemented	Incident Response Plan
A.5.7	Threat Intelligence	Yes	SaaS companies exposed to evolving cloud and cyber threats; requires proactive awareness.	Planned	Risk Methodology
A.5.8	Information Security in Project Management	Yes	Development projects must embed security controls.	Implemented	Secure SDLC Policy

A.5.23	Information Security for Use of Cloud Services	Yes	Cloud-first company; control ensures safe use of third-party cloud platforms.	Implemented	Cloud Security Policy
A.5.34	Protection of Personally Identifiable Information (PII)	Yes	Handling of PII is core to compliance with GDPR & HIPAA	Implemented	Privacy Policy, Data Protection Policy
A.7.1	Physical Security Perimeters	No	Not applicable: NimbusTech does not own or manage data centers; relies on ISO 27001 - certified cloud providers. Risk mitigated through vendor due diligence and contracts.	Not Applicable	Vendor Security Reviews
A.7.2	Physical Entry	No	Offices are leased coworking facilities with building - managed access, excluded from ISMS scope.	Not Applicable	Lease Agreements
A.8.6	Capacity Management	Yes	Cloud capacity planning is required to maintain SaaS availability (99.9% SLA).	Implemented	IT Infrastructure SOP
A.8.9	Configuration Management	Yes	Required for maintaining baseline configurations across cloud and endpoints.	Implemented	IT Operations Procedures
A.8.10	Information Deletion	Yes	Customer and corporate data must be securely deleted when no longer required.	Implemented	Data Retention & Deletion Policy
A.8.11	Data Masking	Yes	Sensitive client data used in test environments must be anonymized/ masked.	Planned	Data Protection SOP
A.8.15	Logging	Yes	Logging critical for investigations and forensic evidence in case of incidents.	Implemented	Logging & Monitoring Policy
A.8.16	Monitoring Activities	Yes	Continuous monitoring/ logging required for SaaS operations and threat detection.	Implemented	Security Monitoring SOP

A.8.23	Web Filtering	No	Not applicable; Control is for general endpoint browsing; SaaS platform does not provide user-facing browsing services.	Not Applicable	Endpoint Security Policy
A.8.28	Secure Coding	Yes	NimbusTech develops its own SaaS platform; secure development lifecycle required.	Implemented	Secure Development Policy
A.8.30	Outsourced development	Yes	Third-party vendors and cloud providers form part of the service delivery chain.	Implemented	Vendor Management Policy

1

Status Summary Table:

Implemented	12
Partially Implemented	1
Planned	2
Not Applicable	3

Closing Statement

This Statement of Applicability will be:

- Reviewed annually as part of ISMS management reviews.
- Updated when significant changes occur to the organization's risk environment, business operations, or Annex A controls.
- Verified through both internal and external audits to ensure continuing applicability and effectiveness.

Approved By :
Amelia Hartman - CEO
Date : August 15, 2025

[1] Controls marked Not Applicable were excluded following formal risk assessment and vendor due diligence.