NimbusTech Solutions, Inc.

Gap Assessment Report

Document ID: NT-ISMS-GAP-001
Version: 1.0
Date: August 15, 2025
Owner: Laura Chen, ISMS Manager
Approved By: Rajesh Patel, CISO

1. Purpose

This document summarizes the results of a gap assessment conducted to evaluate NimbusTech's ISMS alignment with ISO/IEC 27001:2022.

2. Scope

The assessment covers all ISMS components within NimbusTech's SaaS operations, including policies, risk management, cloud infrastructure, incident management, and third-party services.

3. Methodology

- Reviewed ISMS Policy, Risk Methodology, SoA, Risk Register, and Incident Response Plan.
- Compared against ISO/IEC 27001:2022 requirements and Annex A controls.
- Assessment conducted using Annex A control checklist and internal documentation review.
- Gaps rated as:
    - Implemented
    - Partially Implemented
    - Not Implemented

4. Gap Analysis Findings

ISO 27001 Requirements	Current Status	Gap Description	Recommended Action
A.5.1 - Policies for Information Security	Implemented	ISMS Policy documented and approved.	Maintain annual review cycle.
A.5.7 - Threat Intelligence	Partially Implemented	Threat intel process noted but no formal integration.	Establish external intel feeds and reporting workflow.
A.5.23 - Cloud Security	Implemented	Controls defined in Cloud Security Policy	Conduct quarterly cloud audits.
A.6.3 - Contact with authorities	Partially Implemented	Roles identified, but no authority contact list maintained.	Develop and update authority contact directory.
A.7.10 - Physical Entry Controls	Not Applicable	Office in shared coworking space; outside ISMS scope.	Manage via vendor contracts.
A.8.11 - Data Masking	Partially Implemented	Basic masking in test environments only.	Adopt standardized data masking tools.
A.8.15 - Logging	Implemented	Central logging in place.	Expand coverage to all critical apps.
A.8.16 - Monitoring	Implemented	SOC monitoring is active and regularly reviewed.	Continue fine-tuning detection rules.
A.8.28 - Secure Coding	Partially Implemented	Code reviews exist but no formal secure SDLC.	Introduce formal secure coding guidelines and training.
A.8.30 - Outsourced Development	Partially Implemented	Vendor contracts exist but limited security clauses.	Enhance supplier agreements with ISO 27001 clauses.

5. Summary & Next Steps

- Strengths: Strong ISMS Policy, risk management framework, and incident response planning.
- Top Gaps: Threat intelligence (A.5.7), Authority contacts (A.6.3), Data masking (A.8.11), Secure Coding (A.8.28), Outsourced development (A.8.30).
- Next Steps:
    - Formalize and implement missing processes.
    - Update vendor contracts with enhanced clauses.
    - Conduct training for secure development practices.

Approved By:
Rajesh Patel - CISO
Date: August 15, 2025