NimbusTech Solutions, Inc.

Risk Register

Document ID	NT-ISMS-RR-001
Version	1
Date	August 15,2025
Owner	Laura Chen, ISMS Manager
Approved By	Rajesh Patel, CISO

Risk ID	Risk Name	Risk Description	Threat	Vulnerability	Likelihood (1-5)	Impact (1-5)	Inherent Risk Score	Existing Controls	Treatment Decsions	Planned Controls	Residual Risk Score	Risk Owner	Status	Linked SoA Controls
R-001	Customer Database	Unauthorized access to customer PII	External attacker	Weak access controls	4	5	20	MFA, role-based access control	Mitigate	Privileged access mgmt, SIEM logging	8	CISO	In Progress	A.5.1, A.5.2, A.8.34
R-002	Cloud Storage	Data leakage due to misconfiguration	Misconfiguration	Lack of config baselines	3	5	15	Cloud IAM, encryption	Mitigate	Automated config scans	6	IT Manager	Open	A.5.23, A.8.9
R-003	Employee Laptops	Malware via phishing	Malicious actor	Employee awareness gap	4	4	16	Email filtering, antivirus	Mitigate	Phishing simulations, training	9	HR Manager	In Progress	A.5.7, A.8.16
R-004	SaaS Application	Exploitation of insecure code	Hacker	Lack of secure coding	3	5	15	Code reviews	Mitigate	Secure SDLC, pentests	7	Dev Lead	Open	A.5.8, A.8.28
R-005	Backup Systems	Ransomware encrypts backups	Malware	Backups not isolated	3	5	15	Weekly backups	Mitigate	Immutable/cloud backups	6	IT Manager	In Progress	A.8.10
R-006	Test Environment	Leakage of masked test data	Insider	Poor masking	3	4	12	Basic anonymization	Mitigate	Stronger masking tools	7	QA Lead	Planned	A.8.11
R-007	Vendor Services	Vendor mishandles client data	Third-party	Weak oversight	3	4	12	Vendor contracts	Transfer	Security audits, SLA updates	8	Procurement	Open	A.8.30
R-008	HR Records	Breach of employee PII	Hacker	Weak DB security	3	4	12	Password Policy	Mitigate	DB encryption, stricter access	7	HR Manager	Open	A.5.34
R-009	Application Logs	Logs tampered/deleted	Insider	No log monitoring	2	5	10	Basic Logging	Mitigate	Centralized logging, alerts	6	IT Security Analyst	In Progress	A.8.15, A.8.16
R-010	Customer Portal	DDoS Attack disrupts service	Attacker	No mitigation	3	5	15	Cloud WAF	Mitigate	DDoS Mitigation Service	8	IT Manager	Planned	A.8.6, A.8.16
R-011	Finance systems	Fraudulent changes	Insider	Lack of duties separation	2	5	10	Finance checks	Mitigate	Segregation of duties	5	CFO	Open	A.5.2, A.8.15
R-012	Compliance Reporting	Fines for missed reporting	Human error	Incomplete Reports	2	4	8	Manual checks	Transfer	Compliance automation	6	Compliance Officer	Planned	A.5.5
R-013	Email Accounts	Account compromise	Phishing	Weak MFA coverage	3	4	12	Basic MFA	Mitigate	Universal MFA	6	IT Security Analyst	Open	A.5.7, A.8.16
R-014	DevOps Pipeline	Code leaked via outsourced dev	Vendor	Weak vendor contracts	3	4	12	NDAs, vendor screening	Transfer	Secure coding clauses	7	Dev Lead	Open	A.8.28, A.8.30
R-015	Cloud Infrastructure	Capacity overload causes outage	Overuse	No monitoring	2	5	10	Manual Scaling	Mitigate	Automated scaling, monitoring	5	IT Manager	In Progress	A.8.6, A.8.16