Nimbus Harbor Technologies, Inc.

IT Security & Acceptable Use Policy Handbook

v1.0 • Effective February 24, 2026

Purpose. This handbook defines minimum security and acceptable-use requirements for Nimbus Harbor Technologies, Inc. It applies to all employees, contractors, interns, and third parties who access company systems, data, or networks.

Local project note. This document is an original, fictional corporate policy set created for an academic RAG assignment.

Document Owner	Chief Information Security Officer (CISO)
Approved By	Executive Leadership Team
Scope	All endpoints, cloud services, SaaS, and corporate networks
Review Cadence	At least annually, and after significant incidents or control changes
Contact	security@nimbusharbor.example (internal)

Table of Contents

How to use this handbook

Each section contains requirements written as testable statements. For audits, treat “must” as mandatory and “should” as strongly recommended. Where feasible, the company measures compliance through logs, tickets, and configuration baselines.

1. Definitions

Key terms

- **Company systems**: Any endpoint, server, cloud account, SaaS tenant, or network owned or managed by Nimbus Harbor.
- **Confidential data**: Non-public data that could harm customers, employees, or the company if disclosed.
- **Endpoint**: Laptops, desktops, mobile devices, and virtual workstations used to access company resources.
- **Least privilege**: Grant only the minimum access required to perform a job function.

2. Policy Governance

Requirements

- The CISO is the owner of this handbook and must review it at least annually.
- All exceptions must be documented, time-bounded, and approved by Security and the relevant VP.
- Policy changes must be versioned and communicated to all users within 10 business days.

3. Acceptable Use

Allowed use

- Company systems may be used for business purposes and limited incidental personal use that does not interfere with work, violate law, or increase risk.

Prohibited activities (must not)

- Disabling or bypassing endpoint security controls (EDR/AV, disk encryption, firewall).
- Installing unapproved software that requires administrative privileges.
- Using peer-to-peer file sharing or unauthorized remote access tools.
- Accessing, storing, or transmitting illegal content or material that violates harassment/discrimination policies.

Testable controls

- Endpoints must run the standard security agent and report healthy status daily.
- Admin privilege must be restricted to approved roles and tracked in an access system.

4. Access Control & Authentication

Requirements

- All access to production systems must be provisioned through an identity provider (IdP) using SSO where supported.
- Privileged access must be role-based and reviewed quarterly.
- Shared accounts are prohibited unless explicitly approved for a system that cannot support individual accounts.

Access reviews

- Managers must certify access lists for their teams within 10 business days of each quarterly review request.

5. Passwords & Multi-Factor Authentication

Passwords

- Passwords must be at least 14 characters or a passphrase of at least 4 words.
- Passwords must not be reused across company and personal accounts.
- Passwords must be stored only in the approved password manager (no browser-only storage for privileged accounts).

MFA

- MFA is required for all remote access and for any system containing confidential data.
- Phishing-resistant MFA (FIDO2/security keys or equivalent) is required for administrators.

6. Data Classification & Handling

Classes

- **Public**: Approved for public release.
- **Internal**: Non-public operational information.
- **Confidential**: Sensitive business or customer data; requires access controls and encryption.
- **Restricted**: Highest sensitivity (e.g., secrets, credentials, regulated PII).

Handling requirements

- Confidential and Restricted data must be encrypted in transit and at rest.

- Restricted data must not be emailed as attachments; use approved secure sharing mechanisms.
- Secrets (API keys, tokens) must never be committed to Git; use environment variables or a secrets manager.

7. Endpoint & Mobile Security

Baseline

- All endpoints must use full-disk encryption and automatic screen lock after 10 minutes of inactivity.
- Operating system security updates must be installed within 14 days (7 days for critical fixes).
- Endpoints must have EDR/AV enabled and reporting.

Removable media

- Use of USB storage is blocked by default; exceptions require Security approval and device encryption.

8. Email, Messaging, and Collaboration Tools

Requirements

- Company email and chat are business records and may be retained for legal and security purposes.
- Sensitive data should be shared using links with access controls rather than attachments.
- Users must report suspected phishing within 1 hour using the designated reporting method.

9. Remote Access & BYOD

Remote access

- Remote access to internal resources must use the approved VPN or zero-trust access gateway with MFA.
- Split tunneling is disabled unless explicitly approved.

BYOD

- Personal devices may access company email/calendar only if enrolled in mobile device management (MDM) and protected by passcode/biometrics.
- BYOD devices must allow remote wipe of company data.

10. Logging, Monitoring, and Privacy

Logging

- Security logs (authentication, admin actions, and critical system events) must be retained for at least 180 days.
- Production systems must forward logs to the central logging platform within 5 minutes of event generation.

Privacy notice

- The company may monitor and investigate use of company systems to protect customers, employees, and corporate assets.

11. Vulnerability Management & Patch Cadence

Scanning

- Internet-facing assets must be vulnerability scanned at least weekly.
- Critical vulnerabilities must be remediated within 7 days; high within 30 days.

Change tracking

- Remediation must be documented in tickets that include evidence (screenshots/logs) and verification steps.

12. Incident Response (IR)

When to declare an incident

- Suspected credential compromise, malware, data loss, unauthorized access, or service disruption due to security causes.

Response lifecycle

- **Detect** -> **Triage** -> **Contain** -> **Eradicate** -> **Recover** -> **Post-incident review**

Requirements

- Security must acknowledge incident reports within 30 minutes during business hours.
- Containment actions must be logged with timestamps and owners.
- A post-incident report must be completed within 10 business days for medium+ severity incidents.

13. Change Management

Requirements

- Changes to production must be made through approved change tickets or pull requests with peer review.
- Emergency changes must be documented within 1 business day after implementation.
- Rollback plans are required for changes that could impact availability or data integrity.

14. Third-Party & Vendor Security

Requirements

- Vendors handling Confidential or Restricted data must sign a data protection agreement and provide security documentation upon request.
- New vendors must be risk assessed before purchase or onboarding.
- API integrations must use least-privilege scopes and rotate credentials at least annually.

15. Enforcement and Exceptions

Enforcement

- Violations may result in access removal, disciplinary action, contract termination, and/or legal action.

Exceptions

- Exceptions must include: business justification, risk analysis, compensating controls, owner, and expiration date.

Appendix A: Quick Compliance Checklist

Use this checklist for self-audits and onboarding.

- Endpoints encrypted and reporting healthy security agent status daily.
- SSO enabled for major systems; MFA required for remote access.
- Admins use phishing-resistant MFA; privileged access reviewed quarterly.
- Confidential/Restricted data encrypted in transit and at rest; secrets not stored in Git.
- Critical vulns remediated within 7 days; logs retained at least 180 days.
- Incident response acknowledgements within 30 minutes during business hours; post-incident report within 10 business days.

Appendix B: Version History

Version	Date	Author	Notes
v1.0	2026-02-24	Security Team	Initial release for internal use