Information Security and Acceptable Use Policy

Northstar Software, Inc.

Effective date: 2025-01-01 | Owner: People Operations | Status: Active

This policy is intended for internal use. It does not create a contract of employment and may be updated at any time.

1. Purpose

Scope: This policy applies to all Northstar Software, Inc. employees (full-time and part-time) and contractors where noted. Local law may impose additional requirements; where local law conflicts with this policy, the stricter standard will apply unless prohibited.

Definitions: “Employee” refers to active staff on the company payroll. “Manager” refers to the employee’s direct manager or other designated approver. “People Operations” (“People Ops”) refers to HR administrators. “Business days” excludes weekends and company holidays.

This policy sets minimum requirements for protecting Northstar information assets and defines acceptable use of company systems.

2. Data Classification and Handling

Data must be handled according to its classification: Public, Internal, Confidential, or Restricted.

Restricted data includes authentication secrets, customer data covered by contracts, and sensitive employee information.

Confidential and Restricted data must be encrypted in transit and at rest where feasible and accessed on a least-privilege basis.

3. Authentication and Access Control

Multi-factor authentication (MFA) is required for company systems where supported.

Passwords must be unique, strong, and stored in an approved password manager. Sharing credentials is prohibited.

Access requests must be approved by the data owner. Access is reviewed periodically and revoked upon role change or termination.

4. Acceptable Use

Company systems are provided for business use. Limited personal use is permitted if it does not interfere with work, violate policy, or create security risk.

Prohibited activities include: unauthorized software installation, bypassing security controls, accessing inappropriate content, or using systems for illegal activities.

Employees must use only approved tools for storing and sharing company data. Unapproved external storage services are prohibited for Confidential/Restricted data.

5. Endpoint and Network Security

Devices must have up-to-date security patches and endpoint protection. Disk encryption is required for company laptops.

Public Wi■Fi must be used with a VPN where required. Employees must not connect to insecure networks when accessing Restricted systems.

Security incidents (e.g., suspected phishing, lost device) must be reported immediately to the Security team or designated channel.

6. Monitoring and Enforcement

Northstar may monitor systems and logs for security, compliance, and operational needs consistent with applicable law.

Violations may result in access removal, disciplinary action, and legal consequences where applicable.