Remote Work and Cross-Border Work 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 establishes expectations and requirements for remote work, hybrid work, and cross-border work arrangements.

2. Eligibility and Work Arrangement Types

Remote work is a privilege that may be granted based on role requirements, performance, security considerations, and business needs.

Work arrangements: (a) On-site, (b) Hybrid, (c) Remote (in-country), (d) Temporary remote (short-term travel), (e) Cross-border remote (working from another country).

3. Core Expectations

Employees must maintain reliable internet access, a safe and professional workspace, and comply with information security requirements.

Employees must be reachable during agreed working hours and attend required meetings. Time zone changes must be approved in advance.

Performance standards and deliverables remain the same regardless of work location.

4. Cross-Border Work Approval

Working from another country (including for short periods) requires written approval from the employee's manager and People Ops before travel.

Cross-border work may trigger payroll, tax, immigration, export control, and data residency obligations. Approvals will consider these risks.

Unauthorized cross-border work is prohibited and may result in disciplinary action.

5. Equipment, Expenses, and Security

Company equipment must be used for company work unless explicitly approved. Devices must be encrypted and protected with strong authentication.

Employees must use approved VPN and security tooling where required. Storing company data on personal devices or unapproved cloud services is prohibited.

Expense reimbursement follows the Travel & Expense Policy and any remote-work stipend guidelines (if applicable).

6. Privacy, Workspace Safety, and Compliance

Employees must protect confidential information from being overheard or viewed by unauthorized individuals. Use privacy screens when working in public places.

Employees are responsible for maintaining a safe workspace. Work-related injuries must be reported promptly.

Local laws may impose additional requirements (e.g., home office stipends). People Ops will communicate any location-specific rules.

7. Changes, Review, and Revocation

Managers may review remote arrangements periodically. The company may modify or revoke remote work approvals based on business needs, security concerns, or performance issues.

Employees must notify their manager and People Ops of any planned relocation or extended travel that changes the work location.