NB-68-25

Device Encryption Policy

Policy Owner	Chief Information Security Officer (CISO)
Effective Date	September 10, 2025
Next Review Date	September 2026
Classification	Internal Use Only

1. Purpose

The purpose of this policy is to ensure the protection of Northbridge Company’s data assets by requiring full disk encryption on all company-owned computing devices. This policy reduces the risk of data loss, theft, or unauthorized access resulting from lost or stolen devices.

2. Scope

This policy applies to all company-owned desktops, laptops, and mobile workstations; all employees, contractors, interns, and consultants who use Northbridge computing assets; and devices operating on Windows 10, Windows 11, or any future approved operating system.

3. Policy Statement

All company-owned computing devices must use full disk encryption (e.g., Microsoft BitLocker or equivalent). Encryption must be enabled prior to deployment to any employee or user. Devices currently in use that are not encrypted must be remediated and encrypted by March 31, 2026. Exceptions may be granted only by the CISO, documented formally, and reviewed annually.

4. Roles and Responsibilities

CISO: Overall owner of this policy; ensures compliance and monitors implementation.

IT Operations: Implements encryption, manages encryption keys, and ensures devices remain compliant.

Department Managers: Ensure their staff cooperate with IT scheduling and requirements.

Employees: Must not disable, tamper with, or attempt to bypass encryption.

5. Enforcement

Any new device issued without encryption enabled must be reported as a compliance incident. Devices found unencrypted after March 31, 2026 will be removed from the corporate network until encryption is enabled. Non-compliance will be escalated to department leadership and may result in corrective action.

6. Compliance and Review

IT will report monthly encryption compliance percentages to leadership. This policy will be reviewed annually or upon significant changes to technology or regulations.