NB-44-25

Northbridge — IR Playbook — Ransomware

Policy Owner	Security & IR
Effective Date	2025-08-01
Revision	1.0
Classification	Internal Use Only
Applies To	All Employees, Contractors, and Vendors

1. Purpose

This document establishes Northbridge standards for ir playbook — ransomware, enabling consistent execution, compliance, and risk reduction.

2. Scope

This policy/procedure applies to all Northbridge personnel, systems, and third parties involved in the activities covered herein.

3. Roles & Responsibilities

- Policy Owner: accountable for stewardship and annual review.
- IT/Security: implements controls, monitors compliance, and reports deviations.
- Managers: enforce requirements within their teams.
- Employees/Contractors: follow procedures and report issues immediately.

4. Requirements & Procedures

- Immediate isolation, network segmentation, and account disablement.
- Preserve volatile artifacts; capture memory and relevant logs.
- Out-of-band communications; activate restoration via clean backups.
- Post-incident: lessons learned, control gaps, risk acceptance.

5. Compliance & Exceptions

Exceptions must be documented with compensating controls and approved by the Information Technology Director. Non-compliance may result in disciplinary action.

6. Review & Maintenance

This document is reviewed annually and upon material change in risk, technology, or regulation.