Northbridge — Phishing Simulation Schedule

Policy Owner	Training & Awareness
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 phishing simulation schedule, 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

- Quarterly campaigns with varied lures; increasing difficulty.
- Just-in-time training for clickers; track repeat offenders.
- KPIs: open/click/report rates; business-unit comparisons.
- Report trends to leadership; adjust content accordingly.

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.