Cybersecurity Awareness Training Policy & Protocol

1.0 Policy Objective & Scope

The objective of this policy is to mandate annual cybersecurity awareness training for all employees, contractors, and third-party personnel who access company systems or data. This training aims to reduce the risk of security incidents caused by human error, such as phishing attacks, weak password practices, and unauthorized data disclosure, and to ensure compliance with PIPEDA and other applicable Canadian privacy laws.

This policy applies to all full-time and part-time employees, temporary staff, interns, and external contractors working on behalf of the company. It covers all company-owned devices, networks, and cloud services, as well as any personal devices used for business purposes under a BYOD agreement.

2.0 Roles & Responsibilities

- **IT Administrator:** Develops, updates, and deploys the training modules via the SwitchDesk portal; tracks completion rates; manages phishing simulation campaigns; and reports compliance metrics to management.
- **HR Manager:** Coordinates training schedules with department heads; ensures new hires complete training within their first week; maintains training records in employee files; and enforces disciplinary actions for non-compliance.
- **Department Heads:** Ensure their team members attend and complete training sessions; reinforce security best practices during team meetings; and report any observed security concerns to IT.
- **All Employees:** Complete assigned training modules by the deadline; apply learned practices in daily work; report suspicious emails or activities immediately to IT; and acknowledge the company's Acceptable Use Policy annually.

3.0 Core Rules & Guidelines

- All employees must complete initial cybersecurity awareness training within 7 calendar days of hire and annual refresher training thereafter.
- **Training content must cover at minimum:** phishing and social engineering recognition, password hygiene (including use of a password manager), safe internet browsing, mobile device security, physical security of workspaces, and proper handling of sensitive data per PIPEDA.
- Phishing simulations will be conducted quarterly; employees who click on simulated phishing links must complete a remedial training module within 48 hours.
- Failure to complete mandatory training by the deadline will result in a written warning from HR and temporary suspension of network access until training is completed.
- Training records must be retained for the duration of employment plus three years for audit and compliance purposes.

4.0 Step-by-Step Procedure / Workflow

1. IT Administrator reviews the current training curriculum annually and updates modules to reflect emerging threats, regulatory changes, and lessons learned from recent incidents.

2. HR Manager schedules the annual training window (e.g., first two weeks of Q2) and notifies all employees via email and the SwitchDesk announcement board at least 14 days in advance.

3. IT Administrator uploads the training modules (video, quiz, and attestation) to the SwitchDesk learning management system and assigns them to all active users.

4. Employees log into SwitchDesk, complete the training modules, and pass the knowledge check quiz with a score of 80% or higher. They must also digitally sign the Acceptable Use Policy attestation.

5. SwitchDesk automatically records completion status and sends a confirmation email to the employee and a notification to the IT Administrator and HR Manager.

6. IT Administrator runs a weekly compliance report from SwitchDesk and shares it with HR Manager and Department Heads to identify non-compliant employees.

7. HR Manager sends a reminder to employees who have not completed training by the two-week mark, with a new deadline of 7 days.

8. If an employee remains non-compliant after the final deadline, HR Manager issues a written warning and IT Administrator temporarily disables their network access until training is completed.

9. IT Administrator conducts a quarterly phishing simulation campaign using a third-party tool integrated with SwitchDesk; results are tracked per employee.

10. Employees who click on a simulated phishing link receive an automated email with a link to a remedial training module and must complete it within 48 hours.

11. IT Administrator reviews simulation results and remedial completion data, then reports aggregate metrics (e.g., click rate, improvement over time) to the executive team.

12. HR Manager files all training records, attestations, and simulation results in each employee's secure HR folder within SwitchDesk for audit readiness.

5.0 Documentation & Compliance

1. All training completion records, quiz scores, and signed attestations are automatically stored in SwitchDesk under each employee's profile and are accessible to HR and IT for audit purposes.

2. Phishing simulation results are logged in a separate SwitchDesk module, with individual click data anonymized for trend analysis but identifiable for remedial tracking.

3. HR Manager conducts a semi-annual audit of training records to ensure 100% compliance and identifies any gaps in coverage (e.g., contractors not enrolled).

4. IT Administrator performs an annual review of the training content and updates it to address new regulatory requirements (e.g., updates to PIPEDA, Bill 64 in Quebec) and emerging threats.

5. All documentation is retained for the duration of employment plus three years, in compliance with PIPEDA record-keeping requirements, and is backed up to encrypted cloud storage daily.

6. An annual compliance report summarizing training completion rates, simulation results, and remediation actions is presented to the Board of Directors or executive leadership.

Regulatory Disclaimer: This document is a generic administrative template provided for educational purposes. The end-user assumes all liability for reviewing, adapting, and validating all protocols against organizational policies.