FREE TEMPLATE — CANADIAN EDITION

Cyber Incident Response Plan Template

Aligned with the Canadian Centre for Cyber Security (CCCS) Framework

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Purpose	Provide a ready-to-customize incident response plan for Canadian SMBs
Framework Alignment	Canadian Centre for Cyber Security (cyber.gc.ca), NIST SP 800-61
Instructions	Replace all [BRACKETED] fields with your organization's specific information. Review and approve annually.
Version Control	Document version, approval date, and approver name must be recorded on this page.

Document Title	[Organization Name] Cyber Incident Response Plan	**Version**	1.0
Approved By	[Name, Title]	**Approval Date**	[Date]
Next Review	[Date — annually recommended]	**Classification**	CONFIDENTIAL — Internal Use Only

PHASE 1 — PREPARATION

Incident Response Team

- Incident Commander: [Name, Title, Phone, Email]
- Technical Lead: [Name, Title, Phone, Email]
- Communications Lead: [Name, Title, Phone, Email]
- Legal/Privacy Advisor: [Name or Firm, Phone, Email]
- Executive Sponsor: [Name, Title, Phone, Email]
- External IR Support (if engaged): [Vendor Name, Phone, Contract #]

Critical Contacts

- RCMP Cybercrime: 1-888-550-3536
- Canadian Centre for Cyber Security: 1-833-CYBER-88 (report@cyber.gc.ca)
- Office of the Privacy Commissioner: 1-800-282-1376
- Cyber Liability Insurer: [Insurer Name, Policy #, Claims Line]
- Internet Service Provider: [ISP Name, Account #, Emergency Line]

PHASE 2 — IDENTIFICATION

Incident Classification Criteria

- Level 1 — LOW: Isolated malware detection, spam campaign, minor phishing attempt with no data access
- Level 2 — MEDIUM: Confirmed malware infection, unauthorized access to non-sensitive system, service degradation
- Level 3 — HIGH: Ransomware, unauthorized access to personal data, data exfiltration suspected, significant service outage
- Level 4 — CRITICAL: Confirmed data breach involving personal information, complete system compromise, regulatory reporting triggered

Initial Assessment Checklist

- What systems are affected?
- When was the incident first detected?
- What type of incident is suspected?
- Is the incident ongoing or contained?
- Has personal information been accessed or exfiltrated?
- Are regulatory notification timelines triggered? (PIPEDA: real risk of significant harm; PHIPA: real risk of significant harm)
- Has the incident been logged in the incident register?

PHASE 3 — CONTAINMENT

Immediate Containment Actions

- Isolate affected systems from the network — disconnect network cable or disable Wi-Fi
- Do NOT power off affected systems unless instructed by technical lead — forensic evidence may be lost
- Change credentials for all potentially compromised accounts
- Enable MFA on all critical systems if not already active
- Preserve system logs — screenshot, export, or copy before any remediation
- Notify Incident Commander and convene the Incident Response Team
- Engage cyber liability insurer and legal advisor if Level 3 or 4

Evidence Preservation

- Document the incident timeline with timestamps
- Capture screenshots of affected systems
- Export relevant logs (firewall, authentication, email, endpoint)
- Document all actions taken and by whom
- Do not alter or delete any data on affected systems without technical lead approval

PHASE 4 — ERADICATION

Eradication Steps

- Identify root cause of the incident
- Remove malware, unauthorized access, or compromised credentials
- Apply patches or configuration changes that address the root cause
- Scan all systems for indicators of compromise (IoC)
- Verify eradication is complete before proceeding to recovery
- Document all eradication actions with timestamps and responsible party

PHASE 5 — RECOVERY

Recovery Actions

- Restore systems from verified clean backups — confirm backup integrity before restoring
- Rebuild systems from scratch if clean backup unavailable
- Reset all credentials on restored systems
- Re-enable services gradually — monitor closely for 72 hours post-recovery
- Confirm full business operations restored
- Remove any temporary containment measures once recovery confirmed

PHASE 6 — NOTIFICATION

Regulatory Notification (if personal data involved)

- PIPEDA — Report to OPC if breach creates real risk of significant harm. No fixed timeline, but must be prompt. Notify affected individuals if real risk of significant harm.
- PHIPA — Report to IPC as soon as reasonably possible. Notify affected individuals. Log all breaches.
- Quebec Law 25 — Report to Commission d'acces a l'information. Notify affected individuals. 72-hour threshold.
- Retain all breach documentation for minimum 2 years.

Internal & External Communications

- Internal staff notification: [draft template in communications annex]
- Client notification (if applicable): [draft template in communications annex]
- Media/public statement: Legal review required before any public statement
- Insurer notification: Notify within timeframe specified in policy

PHASE 7 — POST-INCIDENT REVIEW

Post-Incident Review Actions

- Conduct post-incident review within 2 weeks of resolution
- Document lessons learned and root cause analysis
- Update this Incident Response Plan based on findings

- Brief executive team on incident, response, and improvements
- Confirm all regulatory notifications have been filed and acknowledged
- Update the incident register with final resolution details
- Schedule follow-up security assessment if warranted

ANNUAL REVIEW & TESTING

This plan must be reviewed annually and tested through a tabletop exercise at minimum once per year. A tabletop exercise involves walking the Incident Response Team through a simulated scenario to identify gaps in the plan and build team familiarity with roles and responsibilities.

- DSIT Professional Services Inc. can facilitate annual tabletop exercises and plan reviews as part of a managed services engagement.
- Book a consultation to discuss incident response planning: dsitpro.com/contact