

QUARTERLY DIGITAL SECURITY & TECHNOLOGY REVIEW

Website & Technology Security Report

This report is prepared for the Board of Directors and summarizes the current state of the organization's digital security posture, identified risks, active policies, and recommended actions.

3	1	0	4
Critical Risks Identified	Security Incident Last 12 Months	Unplanned Downtime Events	Policy Gaps Requiring Action

Executive Summary

The organization's website and digital infrastructure are operationally stable with zero unplanned downtime events in the reporting period. However, a review of access controls, staff procedures, and incident response readiness has identified three critical risk areas and four policy gaps that warrant board attention.

The most significant risks are concentrated in credential management, staff offboarding procedures, and the absence of a formal incident response plan. None of these require significant expenditure to address — they are primarily procedural and administrative in nature.

Board Action Required: Approve the four recommended policies outlined in Section 4 and designate a staff member responsible for digital security compliance.

Section 1 — Risk Register

The following risks have been identified through review of current systems, access logs, and staff procedures.

CRITICAL

Weak & Shared Passwords

Multiple staff accounts use simple passwords. At least two administrator accounts share credentials across personal and organizational use. Shared passwords mean a breach of one account immediately compromises all systems using the same credential.

Likelihood: High **Impact:** Severe

Mitigations:

- Enforce strong password policy (minimum 14 characters, mixed case, symbols) • Deploy a password manager — 1Password Teams or Bitwarden Business (~\$5/user/month) • Audit all admin accounts and require unique credentials for each • Enable two-factor authentication on all accounts with admin access

CRITICAL

Staff Offboarding — No Formal Revocation Process

When staff members leave the organization, there is no documented process for revoking digital access. A review found two former staff members with active credentials to organizational systems including the website, email platform, and social media accounts. This represents an ongoing unauthorized access risk.

Likelihood: High **Impact:** Severe

Mitigations:

- Implement a formal offboarding checklist covering all digital access points • Conduct an immediate audit of all active accounts vs current staff roster • Revoke access within 24 hours of any staff departure • Document all active credentials in a password manager accessible to leadership

CRITICAL

No Incident Response Plan

The organization has no documented procedure for responding to a security incident — including website defacement, data breach, ransomware, or phishing compromise. Without a plan, response time is significantly slower and the risk of compounding damage is high. Quebec Law 25 requires notification of the Commission d'accès à l'information within 72 hours of a qualifying breach.

Likelihood: Medium **Impact:** Severe

Mitigations:

- Develop a one-page Incident Response Procedure document • Define who is contacted first, in what order, and what actions are taken • Designate a staff member as the Security Point of Contact • Test the procedure with a tabletop exercise annually

HIGH

Phishing & Social Engineering Exposure

Staff regularly receive email from external parties including donors, government bodies, and partner organizations. Phishing emails impersonating known contacts are the most common vector for organizational compromise. No formal awareness training has been conducted.

Likelihood: High **Impact:** High

Mitigations:

- Conduct annual phishing awareness training — free resources available through the Canadian Centre for Cyber Security • Configure email authentication (SPF, DKIM, DMARC) — currently partially implemented • Establish a reporting channel for suspicious emails

HIGH

Ransomware & Malware Risk

The organization has no endpoint protection policy. Staff use personal devices for organizational work without managed antivirus or device policies. A single compromised device connected to organizational accounts could propagate ransomware across systems. Recovery from a ransomware event without verified backups averages \$200,000+ for small organizations.

Likelihood: Medium **Impact:** Severe

Mitigations:

- Implement a Bring Your Own Device (BYOD) policy with minimum security requirements
- Verify offsite backup schedule and test restoration quarterly
- Consider Microsoft 365 Business Premium which includes Defender endpoint protection

MEDIUM

Plugin & Software Update Lag

WordPress plugins and themes require regular updates to address security vulnerabilities. Manual update processes depend on staff availability and are frequently delayed. Three plugins are currently running versions with known vulnerabilities (CVEs on file).

Likelihood: Medium **Impact:** Medium

Mitigations:

- Enable managed automatic updates for WordPress core and vetted plugins
- Review and remove unused plugins (currently 12 inactive plugins installed)
- Schedule monthly maintenance window for manual review of update log

Section 2 — Infrastructure Status

Website (WordPress)	Operational	Mar 2026	99.98% uptime last 12 months. SSL valid. CDN active.
Offsite Backups	Active	Mar 2026	Daily backups to separate server. Restoration tested Q4 2025.
SSL Certificate	Valid	Mar 2026	Auto-renew enabled. Expires Oct 2026. No action required.
Email Authentication	Partial	Mar 2026	SPF and DKIM configured. DMARC policy missing — recommend p=quarantine.
WordPress Core	Current	Mar 2026	Running 6.4.3. Auto-updates enabled for minor releases.
Plugin Security Scan	Action Required	Mar 2026	3 plugins with known CVEs. Removal or update pending.
Domain Registration	Active	Mar 2026	Registered through Cloudflare at cost. Renewal: Jan 2027.

Section 3 — Policy & Documentation Status

The following table summarizes the status of key security and operational policies. Gaps are flagged for board action.

Password Policy	Missing	No formal policy exists. Recommend 14-char minimum, no reuse, password manager required.
Staff Offboarding Procedure	Missing	No documented digital access revocation process. Immediate action required — see Risk Register.
Incident Response Plan	Missing	Required under Quebec Law 25. Must designate a Privacy Officer and define breach notification steps.
Website Admin Procedure	Missing	No documentation of who can install plugins, approve updates, or create admin accounts.
Data Retention Policy	Partial	Basic retention guidelines exist. Needs formal documentation and board approval.
BYOD / Device Policy	Missing	Staff use personal devices for organizational work. Minimum security requirements not defined.
Backup & Recovery Procedure	Documented	Offsite backup schedule documented. Restoration tested Q4 2025. Review annually.
Privacy Policy (Public)	Documented	Published at yourorganization.ca/privacy. Reviewed for Quebec Law 25 compliance Mar 2026.

Section 4 — Recommended Board Actions

#	Action	Priority	Effort	Owner
1	Conduct full access audit — active accounts vs current staff roster	Critical	2 hrs	ED + IT
2	Revoke access for departed staff immediately	Critical	1 hr	ED
3	Deploy password manager organization-wide (1Password or Bitwarden)	Critical	4 hrs	IT
4	Approve and distribute Password Policy document	Critical	1 hr	Board
5	Develop and approve Incident Response Plan	Critical	3 hrs	ED + IT
6	Add DMARC policy to email DNS configuration	High	1 hr	IT
7	Update or remove 3 plugins with known vulnerabilities	High	2 hrs	IT

#	Action	Priority	Effort	Owner
8	Document Website Admin Procedure — who can do what, and when	High	2 hrs	IT
9	Schedule annual phishing awareness training for all staff	High	Ongoing	ED
10	Formalize BYOD policy and communicate to staff	Medium	2 hrs	ED

About This Report

This report was prepared by **Jer Chapman**, Web Consultant & Holistic Webmaster, jer@jerchapman.com — jerchapman.com. Jer Chapman has provided web consulting, Linux server administration, and digital security services to non-profit organizations across Quebec since 1998.

Monthly board-ready reports are included as part of the Managed Hosting & Partner Package. Reports are generated automatically from live monitoring data and delivered on the first business day of each month. Policy documentation, security audits, and staff training are available as separate engagements.

This document is confidential and intended solely for the Board of Directors of the named organization. Do not distribute externally.