[REDACT]LABS

RESOURCE / 02

CHARITY CYBERSECURITY

Posture Self-Assessment Checklist for Canadian Charities

A board-ready checklist mapping the 13 baseline controls from the Canadian Centre for Cyber Security to the operational realities of charity and nonprofit work.

TORONTO, ON / 2026

redactlabs.ca

How to use this checklist

This document maps the 13 baseline cybersecurity controls published by the Canadian Centre for Cyber Security (CCCS) to a yes/no/partial format you can complete in 30 to 60 minutes with someone who knows your IT environment.

The output is intended to be brought to your board, your funders, or your insurance underwriter as a starting picture of where your organization stands. It is not a certification or audit; it is a structured self-assessment.

Scoring

For each line item, mark:

- Y — fully in place across your organization.
- P — partially in place.
- N — not in place.
- ? — unsure, needs investigation.

Anything other than Y is a gap worth a conversation. The pattern of gaps usually clusters by team or by system, which makes prioritization easier.

> SOURCE STANDARD
>
> The 13 baseline controls described here are published by the Canadian Centre for Cyber Security at cyber.gc.ca. CCCS designed these specifically for small and medium organizations, prioritizing the highest-leverage controls over completeness.

Control 1: Incident response plan

- We have a written incident response plan that names a coordinator.
- Staff know how to report a suspected incident.
- The plan covers: malware, account compromise, data breach, ransomware, lost device.
- We have at least one offline copy of the plan.
- We have run a tabletop exercise within the last 12 months.

Control 2: Patch operating systems and applications

- All staff devices have automatic OS updates enabled.
- Browsers update automatically.
- Office productivity software (Microsoft 365, Google Workspace, Adobe) updates automatically.
- No staff devices run unsupported OS versions.
- Server / cloud workloads are patched on a documented schedule.

Control 3: Enable security software

- Every staff device runs anti-malware (Windows Defender, macOS XProtect, or commercial EDR).
- Host-based firewalls are enabled.
- Browsers have safe-browsing protections enabled.
- Email gateway scans attachments and links.

Control 4: Securely configure devices

- Default passwords have been changed on every device (including network gear).
- Unused services and ports are disabled or blocked.
- Staff devices use full-disk encryption (BitLocker on Windows, FileVault on macOS).
- Screen locks are enforced (auto-lock after no more than 15 minutes of inactivity).
- Standard staff accounts are not local administrators.

Control 5: Use strong user authentication

- MFA is enforced on email (Microsoft 365 / Google Workspace).
- MFA is enforced on all administrator accounts.
- MFA is enforced on remote access (VPN, RDP, cloud admin consoles).
- We use phishing-resistant MFA (FIDO2 / WebAuthn) for high-privilege accounts.
- SMS-based MFA is avoided where stronger options are available.
- Password policy aligns with current NIST guidance (length over complexity, no forced rotation without compromise).

Control 6: Provide employee awareness training

- Staff complete cybersecurity training within 30 days of hire.
- Annual refresher training is required and tracked.
- We run simulated phishing exercises and use results for coaching, not punishment.
- Staff know how to report a suspected phishing email and reporting is easy.

Control 7: Back up and encrypt data

- All critical data (donor records, financials, programme data) is backed up.
- At least one backup copy is offline or otherwise inaccessible from primary systems (3-2-1 rule).
- Backups are encrypted at rest.
- We have tested restoring from backup in the last 12 months.
- Backup retention is documented and aligns with legal and donor expectations.

Control 8: Secure mobile devices

- Organization-owned mobile devices have a lock-screen passcode enforced.
- Mobile devices have remote-wipe capability (Microsoft Intune, Google Workspace MDM).
- We have a written policy for personal devices accessing organizational data (BYOD).
- Lost or stolen devices have a documented response process.

Control 9: Establish basic perimeter defences

- Office network has a properly configured firewall.
- Wi-Fi for staff requires WPA2 or WPA3 with a strong shared key (or WPA-Enterprise).
- Guest Wi-Fi is on a separate network with no internal access.
- DNS uses a filtering resolver that blocks known malicious domains.

Control 10: Secure cloud and outsourced IT services

- We maintain a list of every cloud service that holds organizational data.
- Each cloud service has MFA enforced for admin accounts.
- Cloud admin access is reviewed at least quarterly.
- Where supported, audit logging is enabled and exported.
- We have data-processing agreements (DPAs) with vendors that hold personal information.

Control 11: Secure websites

- Our website is served over HTTPS with HSTS enabled.
- CMS (WordPress, etc.) and plugins are kept up to date.
- Admin accounts have strong passwords and MFA.
- The website does not collect more donor information than necessary.
- DMARC is published for the email domain to prevent spoofing.

Control 12: Implement access control

- Each staff member has their own user account (no shared accounts).
- Permissions follow least-privilege.
- Departing staff have access removed within 24 hours.
- Administrator accounts are separate from regular accounts.
- Access lists are reviewed at least quarterly for sensitive systems.

Control 13: Secure portable media

- USB ports on staff devices are policy-controlled.
- Portable media containing organizational data is encrypted.
- We have a process for sanitizing or destroying old media.

Charity-specific considerations

The 13 baseline controls are the technical floor. For Canadian charities, three additional considerations sit on top:

Donor data minimization

Collect only the donor information you actually need. Every additional field increases breach exposure, retention obligations under PIPEDA, and Quebec Law 25 disclosure scope.

Board-level cybersecurity oversight

Cybersecurity should appear on the board agenda at least annually. The board should know: who is the named privacy officer, what is the most recent posture assessment, what was the last incident, what is the insurance position.

Privacy law compliance

PIPEDA applies federally. Quebec Law 25 applies if you process personal information of Quebec residents. PHIPA applies if you handle personal health information in Ontario. Each has obligations beyond the technical controls in this checklist.

> WHAT TO DO WITH THE RESULTS
>
> Tally your Ys, Ps, and Ns. Group gaps by theme (identity, devices, vendors). Pick the three highest-impact gaps and build a 90-day plan. Bring that plan to the board with a budget. This is exactly the structure of our charity-tier engagement model.

If you want help

Our charity practice runs this assessment as a fixed-fee Posture Snapshot, with senior-engineer interviews, a board-ready written report, and a prioritized 12-month roadmap.

contact@redactlabs.ca