DVG Systems

A DVG SYSTEMS TOOLKIT · EDITION 2026

The Business Continuity Planner

The plan your cyber insurer, your funders, and your biggest clients will ask to see — not something that lives in a binder no one ever opens. Built for Canadian small businesses and nonprofits.

www.dvgsystems.com · (807) 700-0061 v2026.04

Who actually audits your continuity plan

A common myth: CRA audits IT and continuity controls for charities and small businesses. It doesn't. CRA looks at T3010 filings, receipting, governance, and financial records. **IT and cyber resilience are not on the CRA audit scope.**

The people who *do* ask — and decide whether you keep operating — are these:

- **Cyber insurers** — renewal forms in 2026 ask whether a written BCP exists, when it was last tested, and name specific scenarios (ransomware, cloud outage, key-person loss).
- **Funders** — Ontario Trillium Foundation, United Way, and federal grant programs increasingly ask nonprofits about data handling and continuity on renewal or new applications.
- **Enterprise clients** — vendor-risk questionnaires from hospitals, school boards, municipalities, and mining operators ask you to produce your BCP on request.
- **Your board** — fiduciary duty is now interpreted to include cyber resilience oversight. Directors who can't demonstrate oversight of a BCP are personally exposed.
- **Your donors and your reputation** — after a breach, silence looks like cover-up. A clear communication plan is the difference between recoverable and not.

This planner gives you a 6-section framework a board, insurer, or funder will recognise — and it's short enough to actually finish.

Section 1 — Critical process inventory

List every process the organization cannot go more than 72 hours without. Rate each by **RTO** (recovery time objective — how fast you must be back) and **RPO** (recovery point objective — how much data loss is tolerable).

TEMPLATE

Process	Owner	RTO	RPO	Depends on
Payroll	Finance Lead	< 48h	< 24h	M365, bank portal, ADP
Client billing				
Donor database access				

Section 2 — Data and system inventory

Where does each category of important data live, and who has access?

TEMPLATE

Data / system	Hosted where	Backup location	Access controlled by
Email & files	Microsoft 365	M365 backup tool	Entra ID / MFA
Accounting	QuickBooks / Sage	Vendor native + local export	
Donor / CRM	Salesforce / Raiser's Edge / HubSpot		
Production data			

Section 3 — Dependency map

Which third parties would take your operation down if they failed? Name the vendor, the failure scenario, and your fallback.

TEMPLATE

Dependency	Failure impact	Fallback plan	Workaround lead time
Internet (primary ISP)	All cloud services offline	Mobile hotspot tier / secondary ISP / failover router	< 1h
Microsoft 365	Email, files, Teams all down	Personal Gmail for staff; SMS/call tree for clients	Immediate
Phone system	Inbound calls fail	Forward DID to mobile; SMS banner	15 min
Power	Office unusable	Remote-work posture; UPS on critical gear	Immediate

Section 4 — Roles, contacts, and the call tree

In a crisis, nobody should be looking up contact details.

TEMPLATE

Internal response team

Role	Name	Mobile	Alt email
Incident Commander	Usually the Owner / ED		
IT / MSP Lead			
Communications Lead			
Board Chair			
Legal counsel			

External hotlines (put these on a laminated card)

- **Cyber insurer breach hotline:** _____ Policy #: _____
- **Managed IT provider (24/7):** _____
- **Primary ISP support:** _____
- **Microsoft 365 support (via tenant):** portal.microsoft.com
- **Privacy commissioner (PIPEDA breach, if applicable):** 1-800-282-1376 (OPC)
- **Canadian Anti-Fraud Centre:** 1-888-495-8501
- **Local police (non-emergency):** _____

Section 5 — Incident playbooks (the top 4 for Canadian SMBs)

Playbook A — Ransomware

1. **Isolate:** disconnect affected devices from the network (pull cable or disable Wi-Fi). Do NOT power down — volatile memory holds evidence.
2. **Escalate:** call the cyber insurance hotline first. They appoint the breach counsel and the forensic team — calling your MSP first can invalidate coverage.
3. **Communicate:** staff are told what to say (and what not to say). Clients get the templated breach message within the timeframe your contracts require.
4. **Recover:** restore from immutable backup under the supervision of forensic investigators, not before.
5. **Learn:** within 14 days of recovery, run a post-incident review. Update this plan.

Playbook B — Microsoft 365 outage

1. Check `status.office.com` (tenant) and `admin.microsoft.com` service health.
2. Staff switch to the pre-established fallback (personal Gmail for client communications; phone for urgent internal).
3. Communications Lead posts status to clients — default channel: your website banner + SMS.
4. Log the outage in the continuity journal for insurance and post-incident review.

Playbook C — Key person loss (sudden)

1. Recover access to accounts through the break-glass path (password manager emergency access, Entra ID break-glass account, IT administrator escalation).
2. Notify clients and vendors who had a direct relationship with the person.
3. Reassign in-flight work through the owner list in Sections 1 and 4.
4. Begin offboarding / knowledge-transfer within 5 business days.

Playbook D — Prolonged ISP or power outage

1. Trigger remote-work posture (staff work from home or a cafe with hotspot).
2. Forward office phone lines to mobile or a secondary number.
3. Post status update for clients on website and social.
4. Log outage in continuity journal. Notify insurer if business interruption coverage is in play.

Section 6 — Test schedule and evidence log

A plan you haven't tested isn't a plan. Build the habit below.

Test	Frequency	Evidence kept
Tabletop exercise (one playbook)	Twice a year	Attendance, notes, action items, closure dates
Restore-a-file drill from backup	Quarterly	Screenshot of restored file with timestamp
Full VM / server restore to alternate hardware	Annually	Runbook + screenshots + time-to-recover log
Phone / communications fail-over	Annually	Test call log with before/after screenshots
Contact-tree ping	Annually	Record of who confirmed within the target window

The evidence log matters more than the plan itself. Insurers and funders don't read the binder. They ask for the most recent test log. Keep the last 24 months of evidence in the same folder as the plan.

The one-page summary (for funders, insurers, and enterprise clients)

When a request for your BCP arrives, send this one-pager first. It answers the 10 questions they ask in a format they can copy into their files.

ONE-PAGE BCP SUMMARY — FILL AND SIGN

Organization: _____

Plan date / version: _____

Plan owner: _____ Board reviewer: _____

Critical processes documented: yes / no — count: _____

RTO on highest-priority process: _____

Primary continuity scenarios covered: ransomware · cloud outage · key-person loss · ISP/power outage · _____

Cyber insurance carrier: _____ Policy #: _____

Last tabletop exercise: _____ Next scheduled: _____

Last restore test: _____ Next scheduled: _____

Signed by: _____ Title: _____ Date: _____

Sources

1. Canadian Centre for Cyber Security, "Baseline cyber security controls for small and medium organizations" — cyber.gc.ca
2. Canadian Centre for Cyber Security, ITSAP.40.003 "Developing your IT recovery plan" — cyber.gc.ca
3. Office of the Privacy Commissioner of Canada, "Privacy breach guidelines" — priv.gc.ca
4. Ontario Trillium Foundation, Grant governance requirements — otf.ca
5. Coalition, 2026 Cyber Claims Report — coalitioninc.com/claims-report/2026

Want help turning this into a finished, tested plan?

DVG Systems runs a for Northern Ontario businesses and nonprofits. We help you fill the template, run your first tabletop, and hand you the one-page summary and evidence pack your insurer and funders are asking for.

TALK TO US
(807) 700-0061

EMAIL
solutions@dvgsystems.com

BOOK ONLINE
www.dvgsystems.com/contact