cybersecurityinquiry@accerta.ca

647-438-7857

www.accerta.ca

accerta
Canadian Owned and Operated

Cybersecurity Readiness Checklist

This checklist is intended for use by Indigenous and public sector organizations. For each cybersecurity measure, check the box if it is already in place within your organization.

Governance & Leadership	In place
Cybersecurity is discussed at the leadership or board level.	☐
Roles and responsibilities for cybersecurity are clearly defined.	☐
A cybersecurity strategy or roadmap is established.	☐
Cybersecurity aligns with organizational priorities and risk appetite.	☐
Risk Management	
A cybersecurity risk assessment has been conducted recently.	☐
Critical systems and data are identified and prioritized.	☐
Cyber risks are documented and actively managed.	☐
Third-party risks are assessed and monitored.	☐
Asset & Data Protection	
An inventory of systems and assets is maintained.	☐
Sensitive data is identified and appropriately protected.	☐
Access to systems and data is controlled.	☐
Privileged access is restricted and reviewed.	☐
Technology & Security Controls	
Systems are regularly patched and updated.	☐
Monitoring and logging are in place.	☐
Vulnerabilities are assessed through testing or review.	☐
Devices and remote access are securely managed.	☐
Awareness & Training	
Staff receive cybersecurity awareness training.	☐
Security expectations are communicated clearly.	☐
Training is adapted based on roles and responsibilities.	☐

cybersecurityinquiry@accerta.ca

647-438-7857

www.accerta.ca

accerta
Canadian Owned and Operated

Third-Party & Supply Chain Risk	In place
Vendors are evaluated for cybersecurity risks.	☐
Contracts include appropriate security requirements.	☐
Third-party access is controlled and monitored.	☐
Business Continuity & Resilience	
Business continuity plans include cyber scenarios.	☐
Recovery processes and timelines are defined.	☐
Plans are tested periodically.	☐
Data Governance & Privacy	
Data handling and protection practices are defined.	☐
Privacy requirements are identified and addressed.	☐
Data retention and disposal practices are in place.	☐
Incident Response & Preparedness	
An incident response plan is established.	☐
Roles and escalation processes are defined.	☐
Staff know how to report incidents.	☐
Exercises or simulations are conducted.	☐
Lessons learned are captured and applied.	☐

For additional information or questions, contact us at cybersecurityinquiry@accerta.ca to learn how cybersecurity advisory services can strengthen readiness, governance, and executive oversight.

This checklist is provided for general informational purposes only and does not constitute legal or professional cybersecurity advice.