Please answer the questions below, if you are not sure of the answer, select "No" or leave blank. You are not necessarily expecting you to achieve all the below. We will use the answers to assess your risk profile and match it to our requirements for this project.

1. Policies	
1.1 Are all your employees required to sign an Acceptable Use Policy?	○ [Yes] ○ [No]
1.2 Do all employees receive at least yearly cybersecurity awareness training?	○ [Yes] ○ [No]
1.3 Do you perform regular phish simulation to employees?	○ [At least monthly] ○ [Sometimes] ○ [No]
1.4 Do you perform Third Party Risk assessments for all your vendors that may have access to our data?	○ [Yes] ○ [Sometimes] ○ [No]
1.5 Have you completed a Cybersecurity audit in the last year?	○ [ISO27001] ○ [SOC 2] ○ [Other] ○ [No]
1.6 Have you completed a penetration test (pen test) in the last year?	○ [Yes] ○ [No]
1.7 Do you mandate that all third-party vendors that can access your data or influence your cybersecurity posture to successfully pass an ISO27001 or SOC2 certification yearly?	○ [Yes] ○ [No]
1.8 Do you have a Data Classifications system in place?	○ [Yes] ○ [No]
1.9 Do you have policy to forbid company data (including emails) on personal devices?	○ [Yes] ○ [No]
1.10 Is that policy enforced with tools and/or configurations?	○ [N/A] ○ [Yes] ○ [No]
1.11 Do you have policy to forbid company data on cloud services not managed by the company?	○ [Yes] ○ [No]
1.12 Do you have tools in place to monitor and block sensitive data from leaving the company?	○ [Yes] ○ [No]
1.13 Do you have a mandate to keep all storage and processing of data within Canada?	○ [Yes] ○ [No]
1.14 Do you keep an inventory of all your IT assets?	○ [Yes] ○ [No]
1.15 Do you follow a Zero Trust security approach?	○ [Yes] ○ [No]
1.16 Do you delete sensitive data that is no longer required?	○ [Yes] ○ [No]

1.17 Do you have Cyber “Liability” Insurance?	○ [Yes] ○ [No]
2. Service Levels	
2.1 Do you have Service Levels Agreements (SLA) to guarantee your services to us?	○ [Yes] ○ [No]
2.2 Do those Service Levels Agreements (SLA) have financial penalties attach to them or are those best effort only?	○ [Financial] ○ [Best effort] ○ [No]
2.3 Do you have a formal Disaster Recovery (DR)/Business Continuity Plan (BCP)?	○ [Yes] ○ [No]
2.4 What is the targeted Return To Operations from the Plan?	○ [<24h] ○ [24-48h] ○ [48-72h] ○ [over 72h]
2.5 Do you test the DR/BCP Plan at least yearly?	○ [Yes] ○ [No]
2.6 Do you perform and retain a post test review documenting the results of the plan? [Yes] [No]	○ [Yes] ○ [No]
2.7 Do you have a Cybersecurity Incident Response Plan (CIRP)?	○ [Yes] ○ [No]
2.8 Do you test the CIRP Plan at least yearly?	○ [Yes] ○ [No]
2.9 Does your plan include communicating with your client to advise them of potential breaches?	○ [Yes] ○ [No]
3. Backups:	
3.1 How often do you backup data?	○ [Hourly] ○ [Daily] ○ [Weekly] ○ [Sometimes] ○ [No]
3.2 Are the backups encrypted in transit?	○ [AES 128/256] ○ [Other] ○ [No]
3.3 Are the backups encrypted at rest?	○ [AES 128/256] ○ [Other] ○ [No]
3.4 Is there at least one copy of the data “offsite”?	○ [Yes] ○ [No]
3.5 Are the backups immutable (can someone delete them intentionally or unintentionally)?	○ [Yes] ○ [No]
3.6 Can someone in your organization delete/destroy all backup copies (willfully or unwilfully)?	○ [Yes] ○ [No]

3.7 How often are test data restores performed	○ [At least monthly] ○ [Quarterly] ○ [Yearly] ○ [No]
4. Identity and Access	
4.1 Do you mandate Multi Factor Authentication (MFA) for all cloud based services?	○ [Yes] ○ [No]
4.2 Do you mandate Multi Factor Authentication (MFA) for all remote accesses?	○ [Yes] ○ [No]
4.3 Are identities/logins shared between multiple individuals?	○ [Yes] ○ [No]
4.4 Are dedicated privileged accounts used (dual account policy)?	○ [Yes] ○ [No]
4.5 Do you use a Privileged Access Management (PAM) solution to manage all your privilege accounts?	○ [Yes] ○ [No]
4.6 Does you PAM solution require Multi Factor Authentication (MFA) to access the privileges?	○ [Yes] ○ [No]
5. Technical	
5.1 Are all mobile devices with company data (laptops, smartphones…) configured to enforce encryption to local storage?	○ [AES 128/256] ○ [Other] ○ [No]
5.2 Are all [security] event logs centralized and reviewed at least daily?	○ [Yes] ○ [No]
5.3 Are all user access logs centralized and audited (successful and failed)?	○ [Yes] ○ [No]
5.4 Do you archive all security logs?	○ [1 year or more] ○ [3 months] ○ [1 month] ○ [No]
5.5 Do you use an event correlation tool such as a Security Information and Event Management (SIEM) to identify attack patterns?	○ [Yes] ○ [No]
5.6 Are all security alerts reviewed and acted upon immediately?	○ [Yes, 24/7] ○ [Yes, 8/5] ○ [No]
5.7 Are all devices and servers Operating Systems and Software running versions that are still of supported by their respective vendors?	○ [Yes] ○ [No but isolated] ○ [No]
5.8 Are all critical patches deployed within	○ [1 month] ○ [1 week] ○ [72h] ○ [24h] ○ [No]
5.9 Do you have a process to verify that all critical patches are deployed?	○ [Yes] ○ [No]

5.10 Are all other patches deployed within 30 days of getting released by their vendors?	○[Yes] ○[No]
5.11 How often do you perform vulnerability scans of all your network?	○[At least weekly] ○[Monthly] ○[Yearly] ○[No]
5.12 Are all discovered critical/severe vulnerabilities addressed within	○[1 week] ○[1 month] ○[No]
5.13 Are all other discovered vulnerabilities addressed?	○[1 month] ○[3 months] ○[No]
5.14 Do you inspect all unencrypted traffic between the Internet and your internal devices?	○[Yes] ○[No]
5.15 Do you inspect all encrypted traffic between the Internet and your internal devices?	○[Yes] ○[No]
5.16 Do you have an End Point Detection (EDR) agent deployed to all laptops, desktops and servers?	○[Yes] ○[No]
5.17 Do you have an End Point Detection (EDR) agent deployed to all smartphones?	○[Yes] ○[No]
5.18 Is the EDR agent configured for automatic containment of devices in case of suspected or detected malicious activity?	○[Yes] ○[No]
5.19 Does the anti-malware agent include an isolation/containment feature in case of detected issues?	○[Yes] ○[No]
5.20 Do you block the ability to copy data to USB devices (external drives, thumb drives..)?	○[Yes] ○[No, but must be encrypted] ○[No]
5.21 Do you scan all incoming emails for known and unknown malware (attachments and links) before they are delivered to the user's mailbox?	○[Yes] ○[No]
5.22 Do you scan all outgoing emails for known and unknown malware (attachments and links) before they are delivered to the user's mailbox?	○[Yes] ○[No]
5.23 Do you tag all external emails so that employees can easily identify emails coming from outside your organization?	○[Yes] ○[No]
5.24 Is your email domain setup to strictly enforce SPF?	○[Yes and DMARC] ○[Yes and DKIM] ○[Yes, SPF Only] ○[No]
5.25 Are users setup as regular users on their desktops and/or laptops (not local admin)?	○[Yes] ○[No]
5.26 Do you use network segmentation to separate device and services based on risk profile?	○[Yes] ○[No]
5.27 Are those segments separated by a Next Generation Firewall configured to limit connections to the minimum required?	○[Yes] ○[No]

5.28 Do you use a protective DNS filtering service to monitor and block access to malicious content?	○ [Yes] ○ [No]
5.29 Do you have Intrusion Detection/Prevention System (IPS/IDS) inspecting traffic between internal zones and external zones?	○ [Yes] ○ [No]
5.30 Do you have Intrusion Detection/Prevention System (IPS/IDS) inspecting traffic between internal zones?	○ [Yes] ○ [No]
5.31 Are servers allowed to browse the Internet?	○ [Yes] ○ [No]
5.32 Are unsecured protocols turned off/disabled (telnet, http, TLS 1.0, SSL 3.0…)	○ [Yes] ○ [No]
5.33 Are all vendor default passwords changed?	○ [Yes] ○ [No]
5.34 Are all vendor default accounts disabled?	○ [Yes] ○ [No]
5.35 Do you use a standard hardened baseline configuration on all devices?	○ [Yes] ○ [No]
5.36 Is the hardened baseline regularly reviewed and updated by an information security professional o obtained from a trustworthy service?	○ [N/A] ○ [Yes] ○ [No]
5.37 Is production data forbidden in non-production systems?	○ [Yes] ○ [No]
5.38 Do you follow secure development practices and perform systematic code security reviews?	○ [N/A] ○ [Yes] ○ [No]

I HEREBY DECLARE that the above answers are true and I have not suppressed or misstated any material fact.

Signature:	Date:
Name:	Title:

Do you need help improving your cybersecurity posture? Do you have suggestion to make this questionnaire better? Talk to us: talk@alcit.com