Cyber Audit Checklist

## 1. Access and Identity Management

- Enforce strong password policies (minimum length, complexity, expiration)
- Enable multi-factor authentication (MFA) for all critical systems
- Review and revoke access for former employees or inactive accounts
- Implement role-based access controls (RBAC)

2. Employee Awareness & Training

- Conduct regular cybersecurity awareness training
- Simulate phishing attacks to test employee readiness
- Provide clear policies on acceptable use and data handling

3. Device & Endpoint Security
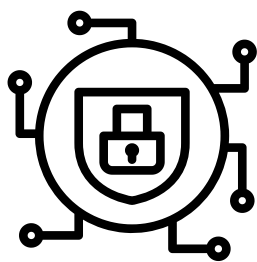
- Ensure antivirus/anti-malware software is installed and updated
- Apply operating system and software patches regularly
- Encrypt all company laptops and mobile devices
- Use mobile device management (MDM) for remote work setups

4. Network & Infrastructure Security

- Secure Wi-Fi networks with strong encryption (WPA3 recommended)
- Use firewalls and intrusion detection/prevention systems (IDS/IPS)
- Segment networks to isolate sensitive systems
- Disable unused ports and services

5. Data Protection & Privacy

- Classify data by sensitivity (e.g., client files, financials, HR)
- Encrypt sensitive data at rest and in transit
- Back up data regularly and test recovery procedures
- Ensure compliance with PIPEDA and other applicable regulations

6.Vendor & Third-Party Risk

- Maintain a list of all third-party vendors with access to your systems or data
- Conduct vendor risk assessments
- Require vendors to meet minimum security standards (e.g., SOC 2)

7. Incident Response & Recovery

- Develop and document an incident response plan
- Assign roles and responsibilities for breach response
- Test your plan with tabletop exercises or simulations
- Maintain a communications plan for clients and regulators

8. Documentation & Audit Readiness

- Keep records of all policies, procedures, and security controls
- Document previous audits and remediation steps
- Assign ownership for each control and track progress
- Prepare a summary report for insurers or regulators