FREE RESOURCE — 2026 EDITION

LSO Cybersecurity Requirements Ontario Law Firm IT Checklist

Everything Ontario Lawyers Need to Know About LSO Cybersecurity Obligations

DSIT Professional Services Inc. | dsitpro.com | Ontario, Canada

Authority	Law Society of Ontario (LSO) — Rules of Professional Conduct, By-Law 9
Applies To	All Ontario lawyers and law firms collecting, storing, or transmitting client information
Key Obligation	LSO requires all lawyers to have a written cybersecurity policy and to take reasonable steps to protect client confidences
Risk	Failure to maintain adequate cybersecurity is a professional conduct matter — reportable to the LSO

LSO CYBERSECURITY OBLIGATIONS — OVERVIEW

- LSO Rule 3.3-1 requires lawyers to protect confidential client information from unauthorized disclosure.
- By-Law 9 requires reasonable measures to protect client property, including electronic records.
- The LSO has published guidance stating that lawyers must have a written cybersecurity policy.
- Firms must conduct regular risk assessments and implement controls proportionate to the sensitivity of client data held.
- Cloud storage of client data is permitted provided adequate security measures are in place and client consent is obtained where appropriate.
- Data breaches involving client information must be reported to the LSO and affected clients promptly.

WRITTEN CYBERSECURITY POLICY — REQUIRED ELEMENTS

Your written cybersecurity policy must address all of the following areas. A policy template follows this checklist.

■ **Acceptable use of firm technology**	Devices, email, internet, cloud	■ **Password requirements**	Length, complexity, MFA mandatory
■ **Remote access controls**	VPN, approved devices only	■ **Client data storage and encryption**	At rest and in transit

■ **Cloud service usage policy**	Approved vendors listed	■ **BYOD (personal device) policy**	MDM enrollment or prohibition
■ **Physical security**	Screen locks, clean desk, visitor access	■ **Incident response procedure**	Breach detection and notification
■ **Staff training requirements**	Annual training documented	■ **Third-party vendor assessment**	Suppliers handling client data
■ **Software patch management**	Update schedule documented	■ **Backup and recovery procedure**	Frequency and testing schedule
■ **Data retention and destruction**	Retention periods by matter type	■ **Social engineering awareness**	Phishing, impersonation scenarios
■ **Annual policy review**	Review date and approver recorded		

TECHNICAL CONTROLS CHECKLIST

■ **MFA on all firm email accounts**	Microsoft 365 / Google Workspace	■ **MFA on all client portals and document systems**	NetDocuments, iManage, etc.
■ **Full disk encryption on all firm laptops**	BitLocker / FileVault	■ **Encrypted email for sensitive client communications**	Secure email gateway
■ **VPN for remote access to firm systems**	Split tunnel disabled	■ **Next-gen antivirus / EDR on all endpoints**	Vendor confirmed
■ **Automatic OS and software patching**	Patch cycle documented	■ **Dark web monitoring for firm email domain**	Credential breach alerts
■ **Automated offsite backup with test restore**	Last restore date recorded	■ **Network segmentation — guest Wi-Fi isolated**	VLAN configured
■ **Firewall with active threat intelligence**	Rule review schedule	■ **Spam filtering and phishing protection**	Email gateway configured
■ **Screen lock policy — 5 minutes or less**	Group policy enforced	■ **Privileged access management**	Admin accounts separate from daily use
■ **Log monitoring and alerting**	SIEM or RMM alerting active		

WRITTEN CYBERSECURITY POLICY — TEMPLATE OUTLINE

Customize this outline with your firm's specific controls and approved tools. This outline meets LSO guidance requirements when fully completed.

- 1. Purpose and Scope — who this policy applies to and why it exists
- 2. Information Classification — how client and firm data is categorized by sensitivity
- 3. Acceptable Use — permitted and prohibited uses of firm technology and devices
- 4. Password and Authentication Standards — minimum requirements and MFA mandate
- 5. Remote Work and BYOD — approved methods for working outside the office
- 6. Data Storage and Encryption — where client data may be stored and how it must be protected
- 7. Cloud Services — approved cloud platforms and vendor assessment requirements
- 8. Incident Response — how to detect, report, and respond to a security incident
- 9. Training and Awareness — frequency, content, and documentation of staff training
- 10. Third-Party Vendors — requirements for suppliers handling client data
- 11. Retention and Destruction — how long client data is kept and how it is destroyed
- 12. Policy Review — annual review process and approval authority
- Appendix A: Approved Cloud and Technology Vendors
- Appendix B: Incident Reporting Contacts and Procedure
- Appendix C: Staff Acknowledgement Form

GETTING HELP

DSIT Professional Services Inc. helps Ontario law firms achieve and maintain LSO cybersecurity compliance — from writing your cybersecurity policy to implementing the technical controls that support it. Our services include policy development, MFA deployment, encrypted remote access configuration, staff training, and annual compliance reviews.

- Book a free legal IT consultation: dsitpro.com/contact

DSIT Professional Services Inc. | help@dsitpro.com | (613) 696-5842 | dsitpro.com | Ontario, Canada | © 2026 All rights reserved.