PDA Legal

Cyber Security Checklist for Law Firms: A Practical Starting Point

Our free, quick-reference checklist offers a high-level sense-check to help your law firm identify key policy and process gaps in your cyber security. It's not a definitive or exhaustive guide, but rather, a tool to prompt critical thinking.

For tailored advice that reflects the specific risks, systems, and legal obligations your firm faces, contact PDA Legal today via 01423 275 365, enquiries@pdalimited.com or visit our website.

- ☐ Maintain a clear understanding of the SRA's Code of Conduct and Accounts Rules about people's money and information.
- ☐ Knowing your reporting obligations, for example, certain incidents of cybercrime involving personal data must be reported to the ICO within 72 hours.
- ☐ Providing regular training for new and existing staff, including follow-ups to check understanding and retention of knowledge on threats such as spear-phishing.
- ☐ Choosing legal software which has a solid reputation within the sector, rather than unknown applications that could introduce harm into your network.
- ☐ Maintaining a register of devices and software used to conduct the work of the firm, irrespective of the ownership of the device.
- ☐ Being clear on which, if any, software or information resources make use of artificial intelligence. This should also include reviews of any supplier or expert use of AI, too.
- ☐ Carrying out periodic cyber security audits of your processes and controls, as well as technical aspects
- ☐ Performing penetration testing to assess the success of security measures.

- [ ] Conducting a risk assessment and gap analysis of your network, applications, and data-handling processes.
- [ ] Making an inventory of your hardware, software, and perform a user privileges review to help identify any unnecessarily exposed assets or potential vulnerabilities.
- [ ] Introducing role-based access controls (RBAC)
- [ ] Accounting for proper patch management and scheduled updates within your IT policy.
- [ ] Forcing routine, regular changing of passwords to remove complacency vulnerabilities.
- [ ] Ensuring that your firm has implemented technical security controls, which should be suitable for the level of risk your firm is exposed to, such as:
    - **Multi-Factor Authentication (MFA):** Enforce MFA on all remote-access points, email, and privileged accounts for RegTech software.
    - **Endpoint Protection Platforms (EPP):** Deploy suitable antivirus/anti-malware on desktops, laptops, and servers.
    - **Network Defences:** Install and configure firewalls, intrusion-detection systems, and secure VPNs across your network.
    - **Encryption Policies:** Encrypt data at rest and in transit, and manage keys securely.
- [ ] Reviewing your premises' physical security, providing physical access to systems, rooms, or devices only to those who need legitimate access.
- [ ] Reviewing your controls and incident response plan after each test or real-life event.
- [ ] Scheduling an annual independent audit with compliance experts, such as PDA Legal.
- [ ] Staying informed with industry updates from bodies such as the SRA.
- [ ] Using the National Cyber Security Centre's "opt-in service" for high-risk individuals.