



25 July 2025

Information Security in Law Firms A Strategic Responsibility

In today's increasingly complex legal and regulatory environment, clients entrust law firms not only with high-stakes matters, but with deeply sensitive information, from commercial secrets and personal data to strategic documentation. As a result, information security has become a critical expectation, not merely a technical feature but a defining component of a law firm's reliability, professionalism, and long-term value proposition. What follows outlines why structured security is no longer optional, how it enhances client confidence, and what practical elements underpin a credible, resilient information protection framework in the legal sector.



The Context: Rising Expectations in a Digital Profession

In an era of digital dependence, law firms handle highly sensitive data, legal documents, commercial strategies, and personal information that demand absolute protection. Information security is no longer seen as a back-office IT concern; it is central to trust, risk, and long-term collaboration.

Governance and Policy: Foundations of Control

Information security begins with governance. A law firm must establish a formal, documented policy that defines its commitment and approach to safeguarding information. This policy must be reviewed regularly and implemented through a clear assignment of roles and responsibilities. Designating a responsible team member is not only good practice but increasingly expected by sophisticated clients. Without strategic oversight, even strong technical controls risk being fragmented or ineffective.

Access, Assets, and Data Integrity

Control over access is fundamental to maintaining confidentiality. Legal professionals routinely manage confidential material, yet in many firms, access to systems or files may not reflect strict need-to-know principles. Role-based access, device encryption, and formal registration of hardware and mobile devices are not optional safeguards, they are minimum expectations. Data



must be protected both in transit and at rest. Security cannot depend solely on individual caution, it must be engineered into how systems are configured and used.

People and Culture: Awareness as Prevention

Technology alone does not protect data, people do. Training is therefore essential. All members, from partners to support personnel, should receive periodic awareness sessions on cyber threats, phishing detection, and proper use of digital tools. Employment contracts should include confidentiality provisions, and termination procedures must deactivate access rights immediately. A firm's security posture is only as strong as its weakest link, and that link is often human. Investing in a culture of security pays long-term dividends.

Preparedness and Recovery: Planning for the Unexpected

A mature security framework includes well-developed response mechanisms. Firms must not only anticipate the risk of cyber incidents but be prepared to respond. Documented Incident Response Plans (IRPs), Business Continuity Plans (BCPs), and Disaster Recovery Plans (DRPs) are essential tools — and must be tested. Clients expect continuity. The ability to respond quickly to breaches, outages, or threats determines a firm's resilience and protects its reputation when things go wrong.

From Compliance to Strategic Advantage

Security frameworks such as ISO 27001 or the GDPR set important benchmarks. But compliance alone is not enough. Increasingly, firms are judged not only on whether they are secure, but whether they can demonstrate it. Information security, when approached strategically, becomes a differentiator. It builds trust with clients, credibility with regulators, and alignment with the digital future of legal services.

At **Saranti and Partners**, we continue to build on security practices, and in doing so, we strengthen our core mission: to provide excellent legal services, securely and responsibly.



Miltos Apostolidis
Executive Advisor | Head of Business Efficiency
mapostolidis@saranti-partners.com
T: +302120216569

*This publication is provided for general informational purposes only
and does not constitute legal or other professional advice.*