POL016 Law Image Data Security Policy

Document ID:	POL016	Document Title:	Law Image Data Security Policy
Original release date:	26/06/2024	Originally released by:	Phil Watson
Current version:	2	Document owner:	Phil Watson
Date of last update:	21/11/2024	Pages:	6 pages (including covers)

law image
Simple. Smart. Strategic.

CONTENTS

DATA SECURITY POLICY

Law Image is committed to providing secure services to you. This policy outlines how we manage your data.

ISO 27001:2022 Certified

Law Image is **ISO 27001:2022** Information Security Management System (ISMS) **certified** and is committed to managing the data by conforming to the ISO 27001:2022 standard. A copy of our ISMS policy can be found at https://www.lawimage.com/about/our-policies/.

Law Image has implemented stringent rules around data management in order to protect our clients from the risk of data loss or exposure.

We also align with the Essential Eight mitigation protocols from the Australian Signals Directorate. Our maturity level is regularly assessed and improved, currently standing at Level 3.

Principles of Data Security at Law Image

Law Image operates according to the following principles of data security:

1. All client data is treated as confidential.
2. All client data is managed with suitable levels of physical and logical security.
3. Law Image controls data throughout the processing workflow, and maintains the full chain of custody.
4. Law Image respects all statutory and legal requirements for data security.

IT Infrastructure Security

At Law Image, we ensure robust IT infrastructure security by aligning with the Australian Signals Directorate (ASD) Essential Eight mitigation strategies.

Our key security measures include application control to prevent unauthorised software execution, regular updates and prompt application of security patches, and disabling macros by default in Microsoft Office to reduce macro-based malware risks. We also implement browser and email client hardening to block potentially harmful content, restrict administrative privileges to necessary users with regular audits, and keep operating systems up-to-date with the latest security patches. Multi-Factor Authentication (MFA) is used for all users accessing sensitive systems or data, and daily encrypted backups of all critical data are stored securely.

Additionally, our data centre security is enhanced by hosting our own on-premises Data Centre, eliminating vulnerabilities associated with third-party hosting services. This Data Centre is safeguarded with advanced physical security measures, including restricted access and surveillance systems.

Physical Security

Our physical security measures further protect our data and IT infrastructure. The entire IT infrastructure and network are segmented and VLAN'ed, enhancing security by isolating sensitive data and systems from general access and reducing the risk of internal and external threats. We retain client data exclusively in our on-premises Data Centre, providing an additional layer of security and privacy. We do not store data on local PC or laptop drives, minimising the risk of data loss or theft, and all data is managed within our own Data Centre, allowing full control over physical security and access protocols.

Personnel Security

Law Image conducts thorough employment screening, including identity and working rights verification, professional reference checks, and Australian Criminal History Checks before offering employment.

Ongoing employment is contingent on eligible working rights, adherence to company policies including Privacy, Confidentiality, and Code of Conduct, and completion of regular training. Law Image obtains additional certifications, including Anti-Money Laundering (AML) and Federal security clearances, whenever necessary.

Law Image does not subcontract any work to third parties. Law Image does not use external couriers. We do our own pickups and deliveries to maintain security. Law Image maintains the full chain of custody at all times while documents are in our possession.

Incident Management

Law Image ensures a consistent and effective approach to handling Information Security Incidents. All incidents are promptly reported to the National IT Manager, assessed for severity, and managed proportionately. Serious incidents are recorded in the Corrective Action and Business Risk Registers, with new risks promptly mitigated through established risk management processes. Responsibilities for incident reporting and response are clearly outlined, with compliance enforced through internal procedures and contractual obligations with third parties.

Business Continuity Plan

The Business Continuity Plan at Law Image ensures our operations continue during and after critical incidents by following the Prevention, Preparedness, Response, and Recovery (PPRR) framework. It includes regular risk assessments, prioritisation of critical business functions, immediate response strategies, and detailed recovery actions. In case of major disruptions, temporary production facilities and equipment are arranged through a third party, with work coordinated across our offices. Adequate insurance is in place for various risks, and critical activities are identified to prevent severe business impacts from delays. Incident response roles are defined, with a National IT Manager leading the team and managing responses. Regular data backups are securely archived offsite, ensuring data security and continuity.

Data Retention

Data retention follows our Data Classification and Retention policies, varying according to the services requested or as specified by clients. Data is securely deleted using industry best practices, with destruction certificates available upon request.

1. Data retention period

By default, Law Image retains data on the processing server for 14 calendar days after assignment closure.

2. Data deletion after 14 days

After 14 days Law Image runs a file deletion utility to ensure data is completely removed from the server. This utility is compliant with deletion standard DoD 5220.22-M. Alternatively, Law Image can promptly delete data after it has been delivered to clients, upon request.

3. Exclusions from backup

The processing server is not included in the backup regime. This is a security measure, so we do not create additional copies of documents.

4. Secure FTP site

Law Image provides a secure FTP service for uploading and downloading of client files. This system is purely transactional. These files are removed once they are retrieved, and the disk utility is then run to ensure their complete removal. This server's storage is also excluded from the backup regime.

5. Mobile media

Law Image has disabled USB ports on local machines and does not allow the use of USB drives or portable hard drives.

6. No local storage

Law Image's processing terminals have no local storage. All files are kept on the processing server.

7. Encryption

Law Image encrypts all user data at rest using the AES-256 algorithm. All output files sent by Law Image to clients are zipped and password protected.

8. Managing sensitive data

Law Image frequently manages extremely sensitive and protected data for clients. We do not create copies of this data. It is transferred from the S-FTP site, printed, and then immediately deleted from the printer's memory.

POLICY UPDATES

This Policy may change from time to time and is available on our website.

Data Security Policy Enquiries

Please contact Philip Watson (Head of Information Security) directly at pwatson@lawimage.com if you would like further information about how we handle and process your documents.