# Information Security Standard

This Information Security Standard (or "Standard") sets forth the information security standards implemented by Law Debenture with respect to the confidentiality, integrity and availability of information.

### Information Security Policies and Procedures

Law Debenture has and maintains documented information security polices, standards and procedures to establish its control environment related to the protection of confidentiality, integrity and availability of information. Policies and procedures are reviewed, updated, and approved by senior management on at least an annual basis. Policies, standards and procedures are aligned to ISO 27001.

### Governance and Training

Law Debenture have implemented governance arrangements for the management of information security with security responsibilities allocated, controls are implemented and the operation of information security within Law Debenture is undertaken.
All Law Debenture staff complete information security training including, but not limited to, data protection and secure handling of information on an annual basis with senior management oversight on completion of training. All new starters complete their training as part of their onboarding. Security awareness training is provided to staff on a regular basis.

### Human Resources Security

Pre-employment screenings, including criminal background checks (where permitted under local law), review of curriculum vitae, review of credentials and experience are undertaken prior to commencement of employment.

All employees are subject to confidentiality obligations as part of their employment contract. The contract also includes provisions such as, but not limited to:

- Confidentiality obligations post-employment.
- Compliance with all Law Debenture policies and procedures, including data protection policy, information security policy, and IT acceptable use policies concerning the use of electronic resources in a professional, lawful and ethical manner.

Processes are in place to identify and collect assets (physical and electronic) from employees on departure when use is no longer required.
Third-parties, e.g. suppliers, contractors and consultants, advisors, are subject to confidentiality obligations as part of the service agreement signed with Law Debenture.

### Access Control

Law Debenture has a formal approval process to grant access on a least-privilege-basis to fulfil roles and responsibilities. Segregation exists between request, approval and granting of access.

User accounts for access to systems, services and applications are assigned to individual users and not shared. Strong passwords are required to be used with additional controls such as periodic expiration, password age, prevention on reuse of historical passwords, account lockouts. Multi-factor authentication is enabled for remote access.

Privileged and/or administrative user accounts are different to standard user account with greater password controls than user accounts and with multi-factor authentication enabled for all access. Privileged and/or administrative user accounts are restricted to authorised staff and assigned to an individual for their sole use.

Law Debenture deactivates access when no longer needed, e.g. for leavers, change of role in a timely basis. Periodic reviews are undertaken on user accounts without recent activity.
Law Debenture undertakes regular user access reviews to systems, applications, network devices transmitting, storing or processing information belonging to or entrusted to Law Debenture.

### Network and System Security

Law Debenture has, as a minimum, the following network and system security controls in place for information belonging to or entrusted to Law Debenture:

- Hardening standards for operating systems, applications, and network devices based on CIS frameworks.
- Operating systems, applications and network devices are maintained to recommended manufacturer recommended release levels. Vulnerabilities categorised as either critical or high risk are patched in timescales recommended by UK's National Cyber Security Centre.
- Operating systems, applications and network devices are maintained at releases that allow latest security patches/service packs to be applied.

*Network Security Controls:*

- Firewalls with policies are implemented on all networks interfaces that restrict inbound and outbound traffic based on need.

- Intrusion detection and intrusion prevention systems are implemented to detect and respond to unauthorised or malicious network traffic.
- Distributed Denial of Access (DDoS) protection is in place.

*Systems Security Controls:*
- Endpoint devices (laptops) are hardware encrypted and secured with a strong password available to authorised staff only.
- Mobile endpoints (smartphones, tablets) are encrypted and managed using a mobile device management system.
- Servers and endpoints are secured with industry leading endpoint protection including, but not limited to, malware protection, user behaviour monitoring, removeable media management. Access to removeable media is prohibited by default and granted only on business need.

### Logging and Monitoring
Logging activities are documented and performed in accordance with industry security standards with monitoring of user access to identify cybersecurity events and verify the effectiveness of protective measures.

### Threat and Vulnerability Management
Law Debenture undertakes regular vulnerability assessment and timely remediation process for operating systems, applications, and network devices. Our processes identify, assess, mitigate, and protect against new and existing security vulnerabilities and threats from threat intelligence partners.

Law Debenture undertakes regular independent penetration tests on its networks and applications that handle information by CREST approved security companies.

We use a risk-based remediation program to resolve findings from penetration tests, vulnerability scans and compliance assessments.

### Change Management
Law Debenture has implemented a documented change control policy that includes:
- Approval, classification, testing, implementation and back out plan requirements.
- Segregation of duties among request, approval, and implementation.

### Asset Management
Law Debenture maintains an asset inventory, including system/device and software assets for information belonging to or entrusted to Law Debenture.

Law Debenture has asset disposal controls in place to ensure information (hard copy and electronic) is disposed of according to industry standard security standards when no longer needed.

### Information Handling
Law Debenture has documented its approach to the categorisation of information in relation to its confidentiality and sensitivity, and defined rules for the handling of each category of data to ensure the appropriate level of confidentiality, integrity and availability of that information.
Controls have been implemented according to the classification of information to monitor and detect potential information loss or unauthorised access to information.

### Encryption
All information transmitted to or from Law Debenture is encrypted using industry recognised security standards. Information belonging to or entrusted to Law Debenture is encrypted at rest. Backups containing information are encrypted.
Encryption algorithms are industry recognised security standards. Encryption keys owned or managed by Law Debenture are stored securely with access managed and restricted to authorised staff.

### Physical Security
Process and physical controls are in place to protect hard copies and information systems (e.g., hardware, software, documentation, and data) when Law Debenture has information belonging to or entrusted to Law Debenture.
Data centres utilised by Law Debenture have physical controls to manage access to authorised personnel only. Controls include, but are not limited to, CCTV, 24/7 monitoring a to protect data and services from unauthorised access as well as environmental threats. All data centres are surrounded by security perimeters with restricted access controls. Data centres have environmental controls (temperature, humidity, redundant power) to prevent disruptions or loss.
Regular independent physical security assessments of facilities that transmit, store or process information are obtained by Law Debenture for review and assessment.

### Information Destruction
Law Debenture has processes in place to ensure information (hard copy and electronic) is securely destroyed when no longer required using industry standard security standards.

### Information Security Incident Response, Management and Reporting
Law Debenture has security incident (e.g., exposure, breach, theft, etc.) management and response procedures that allow for reasonable detection, investigation, response, remediation/ mitigation and

root cause of events that involve a threat to the confidentiality, integrity and/or availability of information belonging to or entrusted to Law Debenture. Our incident response and management procedures are documented, tested, reviewed at least annually and widely communicated to Law Debenture staff.

Law Debenture has documented notification procedures in place in the event of needing to notify Clients to have entrusted their information to Law Debenture.

**Subcontractor Management**

This Information Security Standard is applicable to all subcontractors utilised by Law Debenture that handle information belonging to or entrusted to Law Debenture. Subcontractors include, but are not limited to, off-site storage third party supplier, cloud hosting facilities and data centre facilities.

Formal contracts between Law Debenture and subcontractors are in place that outline the controls to be provided, including controls to maintain the confidentiality, availability, and integrity of information.

Initial and on-going assessments is conducted to ensure subcontractors are adhering to Law Debenture's Information Security Standard and security incidents and problems are managed appropriately.