Lex Mundi
World Ready

Updated January, 2020

Cyber-Security Core Standards for Member Firms

As per the Service Standards, member firms must meet these Core Standards and use their best efforst to implement the Cyber-Security Recommended Practices.

Note: A firm that is ISO/IEC 27001:2013 certified has met the core standards.

Governance

- One or more members of the firm's governing body or senior leadership group have been identified as accountable for the firm's cyber-security.

Policies

- The firm has an electronic-data security policy that addresses cyber-security issues of the firm's digital information based on access rights that follow the principle of least privilege and includes the roles and responsibilities of lawyers, staff, contractors and third parties who handle confidential or legislatively restricted firm and client information.
- The firm has a physical-data security policy.

Plans

The firm has the following annually-reviewed plans:

- Cyber-security risk assessment and mitigation
- Incident response
- Back-up and restoration
- Business continuity
- Vendor / third-party access management

User Awareness

- All personnel having access to the firm's systems have annual cyber-security awareness training.
- User awareness and understanding is tested using simulated phishing attempts periodically based on the risk for key target groups (at least annually for all users).

Passwords / lock-out

- All devices with access to confidential information are password protected.
- All devices with access to confidential information lock after a period of user inactivity (for example, no longer than 15 minutes).

Encryption

- The firm is able to encrypt critical data in accordance with applicable regulatory or client requirements.
- All encryption is a minimum of AES 256-bit.
- Encrypt data in-transit including email (except where recipient systems do not permit or client representatives indicate otherwise)

Information access control

- Data access controls are in place, including the categorization of data with the assignment (and revocation) of access rights.

Patching / updates

- Patch management is in place so that all servers, workstations, databases, applications and websites are patched on a regular basis, taking into account the criticality of the update.
- Anti-malware software is in place and updated regularly (hourly if possible).
- Anti-virus software is in place and updated regularly (hourly if possible).

Business continuity, backup and restoration

- Appropriate data is backed-up regularly and held securely in a physically-separate location.

Technology

- Firewalls with restrictive settings are in place for critical systems.
- The firm's public wireless network is segregated from the firm's own wireless network.
- Firewalls run a locked down configuration with only required ports opened. Ports should only be opened if there is a clear need.