Lex Mundi
World Ready

Updated January, 2020

Cyber-Security Recommended Practices

These recommended practices provide guidance as to recommended steps to take beyond the Lex Mundi Cyber-Security Core Standards.

Note: all the following practices are under consideration for future inclusion in Lex Mundi's Cyber-security Core Standards.

Plans

- The firm has a data loss prevention plan which is reviewed annually.
- There is an annual review and testing of the firm's back-up and restoration plan.

User Awareness

- User awareness and understanding is tested using simulated threats.
- Users who act appropriately in response to a cyber-security threat (either real or as part of a test) are recognized and / or rewarded.

Passwords / lock-out

- Passwords (memorized secret authenticators), that are unique to each device, are of such length, complexity, duration and/or other attributes (set and controlled by the firm) to be reasonably expected to secure access to data.
    - For more see: Appendix A of NIST Digital Identify Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html#appA
- All devices with access to confidential information:
    - Lock after a period of user inactivity (no longer than 15 minutes)
    - A limited number of unsuccessful login attempts

Encryption

- Encrypt any device or databases with confidential data.
- Encrypt data in-transit including email (except where recipient systems do not permit or clients direct otherwise).
- Mail gateways automatically use transport layer security (TLS) where the remote gateway supports such functionality.
- Mobile devices are secured with Mobile Device Management (MDM) or Mobile Application Management (MAM) software

Business continuity, backup and restoration

- Backup data sets containing confidential information are encrypted, off-line and held at a separate location.

Information access control

- The firm uses role-based access control for all confidential information.
- Information that is no longer required to be retained by law, regulation, client request, or business use is regularly and securely deleted.
- There is an annual audit of administrator accounts which have access to confidential information.

Patching / updates

- All servers, workstations, databases, applications and websites are patched using automation.
- Anti-virus software is in place and updated hourly.
- Anti-malware software is in place and updated hourly.

Vendor / contractors management

- Ensure agreements - including clear responsibilities for reporting and containment in the event of a breach - are in place in advance of a vendor / third-party gaining access to the firm's data
- There will be an annual request of information, from vendors and contractors who have access to confidential data, regarding their cyber-security capabilities and the privacy / security training they provide their staff and contractors.

Assessment and testing

- Ongoing vulnerability assessment - likely quarterly and after a significant change or upgrade.
- Annual penetration testing; more frequently based on an assessment of the firm's risk (e.g. significant externally facing infrastructure)

Insurance

- The firm has cyber / data breach insurance to cover costs for notifying clients, interruption to business, investigation(s) of the breach, and to cover any penalties which might be assessed.

Multi-factor authentication

- Multi-factor authentication (MFA) to be used for remote or off-premise access to the corporate environment and shared virtual resources (e.g. virtual data rooms) via VPN or other similar mechanism.
- MFA should be used whenever feasible (especially to secure confidential / sensitive data). If a user logs in within the firm's firewall, a second level password is sufficient.

Browser cookies

Should be:

- Tagged to be accessible only on secure (HTTPS) sessions
- Accessible to the minimum practical set of hostnames and paths
- Tagged to be inaccessible via JavaScript (Http Only)
- Tagged to expire at, or soon after, the session's validity period

Background checks

- A background check is conducted on all individuals with access to confidential information who are hired as IT / cyber-security staff or as independent contractors.