IT Security and Cyber Hygiene Requirements for Licensed Moneylenders

Measure	Implementation Action
1. Equip employees with the know-how to be the first line of defence	
Register your Data Protection Officer (DPO) via ACRA BizFile+ and make available your DPO's business contact information publicly.	The moneylender should appoint and register a DPO (approved by senior management) to ensure effective internal controls and risk management practices implemented to achieve security, reliability and resilience of its IT operating environment (i.e. data protection and cybersecurity). Moneylender should register with the PDPC https://www.pdpc.gov.sg/overview-of-pdpa/dataprotection/business-owner/data-protection-officers
2. Establish organisation's data protection and security governance policies	
2. Ensuring technology in use is able to address current and emerging threats	The moneylender should establish the technology risk management framework: (a) Roles and responsibilities in managing technology risks; (b) Identification and assessment of impact and likelihood of current and emerging threats, risks and vulnerabilities; (c) Implementation of appropriate practices and controls to mitigate risks; and (d) Periodic update and monitoring of risk assessment to include changes in systems, environmental or operating conditions that would affect risk analysis.
3. Control access to the organisation's data and services	
3.1. Implement Data Security and Protection measures	3.1.1. The moneylender should establish a process to protect its personal data (e.g., password protected documents, encryption of personal data (at rest) and/or emails, enable database encryption). Refer to the DPE Configuration Guide for details (https://www.imda.gov.sg/-/media/imda/files/programme/dpe/dpe-configurationguide.pdf).

	3.1.2. The moneylender should secure its digital online services and data exchange channels with its vendor or partners to protect personal data. This can be achieved through data encryption and digital signatures.
	3.1.3. The moneylender or through their IT vendor should only make available mobile applications or software to customers through official mobile application stores, or other secure delivery channels.
	3.1.4. The moneylender should ensure that employees install/access only authorised software/attachments within the organisation from official or trusted sources.
	3.1.5. Before disposing any paper-based (hard copy) media, the moneylender should carry out steps to ensure that those containing personal, confidential and/or sensitive data have been securely shredded.
3.2. Implement Virus and Malware Protection	3.2.1. The moneylender should use and install Antimalware solutions in endpoints to detect attacks on the organisation's environment. Examples of endpoints include laptop computers, desktop computers, servers and virtual environments.
	3.2.2. Virus and malware scans should be carried out to detect possible cyberattacks. Where feasible, scans should always be automated and remain active to provide constant protection. This includes files and attachments downloaded from the Internet through the web browser or email and external sources such as from portable USB drives.
	3.2.3. The moneylender should enable auto-updates or configure the anti-malware solution to update signature files or equivalent *(e.g., non-signature-based machine learning solutions)* to detect new malware. Where possible, these updates should take place at least daily to stay protected from the latest malware.
3.3. Implement Firewall Configuration	Firewalls should be deployed or switched on to protect the network, systems, and endpoints such as laptops, desktops, servers, and virtual environments. In an environment where there is an organisation's network setup, a network perimeter firewall should be configured to analyse and accept only authorised network traffic into the organisation's network. <u>Application Security</u> Use a web application firewall ("WAF") to defend against typical web application attacks such as SQL injection and XSS attacks. They can act as another layer of security in addition to the application code level.

3.4. Implement Access Control Management	The moneylender should have a process to grant and revoke access with the necessary approvals. The moneylender may implement this requirement in different ways, e.g., email approval or access request form. This should be implemented when there are personnel changes such as onboarding of new staff or change of role(s) for employees. The following fields should be captured: a) Name; b) System to Access; c) Department; d) Role/Account Type; e) From Date; And f) To Date. The moneylender can refer to the Data Protection and Security Policy template (Clause 4.2.1 - Access Control) as a reference (https://go.gov.sg/dpsecurity-policy). In particular, cover the following: (a) Implement role-based access control to limit employee access to job-essential information and systems only. (b) Disable or remove outdated access rights, shared accounts, duplicate accounts, and invalid accounts promptly. (c) Restrict administrator account usage to approved administrative functions with senior management authorisation only. (d) Implement restricted access for third parties/contractors based on job requirements, with immediate removal when access is no longer needed. (e) Enforce physical security measures through cable locks and card access to protect IT assets and environment from unauthorised access. (f) Implement account lockout after multiple failed login attempts through rate limiting or disabling accounts (e.g., after 10 failures). The moneylender can refer to the Data Protection and Security Policy template, Annex F - Account Inventory (Template), as a reference (https://go.gov.sg/dpsecuritypolicy).

3.5. Implement Password Protection	Where feasible, 2-factor authentication (2FA)/multiple factor authentication (MFA) should be used for administrative access to important systems, such as an Internet- facing system containing sensitive personal data. The moneylender may implement this in different ways, e.g., use of an authenticator application on the mobile or one-time password (OTP) token.
3.6. Implement Patch Management/Software Update	The moneylender should prioritise the implementation of critical or important updates for operating systems and applications (e.g., security patches) to be applied as soon as possible. The moneylender can refer to the Data Protection and Security Policy template (Clause 4.2.4 - Configuration Management) as a reference (https://go.gov.sg/dpsecurity-policy).
3.7. Assess third party's cybersecurity readiness	The moneylender should assess and document the cybersecurity posture of all third-party vendors handling sensitive or confidential information. The assessment should include: (a) Cybersecurity certifications (e.g., ISO/IEC 27001); (b) Whether the vendor has experienced recent security incidents or breaches; (c) Use of encryption, access control, and data protection controls; and (d) Cloud security controls, if applicable. Assessment results should influence access provisioning and contractual terms. The moneylender can refer to the following: (a) Annex I – Third Parties Data Protection Agreement; https://go.gov.sg/dpsecurity-policy. (b) CSA Cyber Essentials Toolkit; https://www.csa.gov.sg/enterprise-toolkit.

3.8. Implement security monitoring and logging controls	3.8.1 The moneylender should enable security logging on all critical systems, including: (a) Administrative actions (b) Login and logout events (c) File access and data export attempts (d) Configuration changes Logs must be protected from tampering and reviewed regularly (e.g., monthly). Alerts should be configured for suspicious activity (e.g., failed logins, out-of-hours access).
	3.8.2. Logs must be retained for at least 6 months. Longer retention is encouraged where feasible, especially for systems storing personal or financial data.
	3.8.3 Where feasible, outsource logging review to IT vendor with clear SOP for escalation of suspicious events.
4. Incident response – Be ready to detect, respond to, and recover from cybersecurity incidents	
Develop an Incident Response and Data breach Management Plan	The moneylender should establish an up-to-date basic incident response plan to guide the organisation on how to respond to common cybersecurity incidents. Examples include phishing, data breach, ransomware. The plan should contain details as follows: (a) Clear roles and responsibilities of key personnel in the organisation involved in the incident response plan process. (b) Procedures to detect, respond, and recover from the common cybersecurity threat scenarios, e.g., phishing, ransomware, data breach. (c) Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management). The moneylender may refer to the Data Protection and Security Policy template, Annex G - Incident Response Plan (Template), as a reference (https://go.gov.sg/dpsecurity-policy).