DATA PROTECTION AND CYBERSECURITY GUIDELINES

Measure	Implementation Action
1. Equip employees with the know-how to be the first line of defence	
1.1. Register your Data Protection Officer (DPO) via ACRA BizFile+ and make available your DPO's business contact information publicly.	The moneylender should make the business contact information of the DPO available to the public.
1.2. Complete the Cybersecurity Awareness and Training	1.2.1. The moneylender should put in place cybersecurity awareness training for all employees to ensure that employees are aware of the security practices and behaviour expected of them. The moneylender may meet this requirement in different ways *(e.g., provide self-learning materials for employees or engaging external training providers)*: (a) The moneylender should have a programme in place requiring all personnel to undergo IT security awareness training on a regular basis. The training programme should be reviewed periodically to ensure its contents remain current and relevant. (b) The content of the training programme should minimally include information on the prevailing cyber threat landscape and its implications, as well as an individual's responsibility to safeguard borrower information. The moneylender may refer to the following training materials for employees: CSA Cybersecurity Toolkit for Employees (https://www.csa.gov.sg/employee-toolkit)

	1.2.2. Cyber hygiene practices and guidelines should be developed for employees to adopt in their daily operations. In particular, cover the following: (a) Employees must use only trusted network connections (mobile hotspot, Wi-Fi, VPN) when accessing organisational data or email. (b) Employees must report suspicious emails/attachments to IT team/management immediately. (c) Moneylender must report phishing attempts to authorities and alert customers with protective measures. The moneylender can refer to the Data Protection and Security Policy template (Clause 4.2.6 – IT Acceptable Use Policy) as a reference (https://go.gov.sg/dpsecuritypolicy).
2. Know what data the organisation has, where they are, and secure the data	
2.1. Establish an Asset Inventory for your personal data	2.1.1. The moneylender should identify and maintain an inventory of personal data in the organisation. The moneylender may meet this requirement in different ways, e.g., using spreadsheet or asset inventory software.
	2.1.2. The inventory list shall contain details of the data as follows: (a) Information on purposes for the collection, use and disclosure of personal data, third parties who handle personal data under the organisation's possession or control; (b) Data classification and/or sensitivity; (c) Location; and (d) Retention period. The moneylender may refer to the Data Protection and Security Policy template, Annex B - Asset Inventory Map (Template), as a reference (https://go.gov.sg/dpsecurity-policy).
3. Know the hardware and software that organisation has and protect them	

3.1. Establish an IT Asset Inventory for your hardware and software	3.1.1. The moneylender should identify and maintain an up-to-date asset inventory of all the hardware and software assets in the organisation. The moneylender may meet this requirement in different ways, e.g., use of spreadsheet or IT asset management software to maintain the IT asset inventory. The moneylender can refer to the Data Protection and Security Policy template, Annex B - Asset Inventory Map (Template), as a reference (https://go.gov.sg/dpsecuritypolicy).
	3.1.2. Software assets may include software applications used by the organisation. If the software is hosted in a cloud environment, the moneylender shall include what is hosted on the cloud instances (*e.g., software and Operating System (OS)).*
3.2. Establish an Inventory of Accounts	3.2.1. Account management shall be established to maintain and manage the inventory of accounts. The moneylender may meet this requirement in different ways, (*e.g., using of spreadsheets or exporting the list from software directory services).*

	3.2.2. The account inventory list shall contain details for user, administrator, third-party, and service accounts not limited to the following:
	(a) Name;
	(b) Username;
	(c) Department;
	(d) Role/account type;
	(e) Date of access created; and
	(f) Last logon date.
	The moneylender may refer to the Data Protection and Security Policy template, Annex F - Account Inventory (Template), as a reference. (https://go.gov.sg/dpsecuritypolic y).

4. Establish organisation's data protection and security governance policies	

4.1. Develop a Protection and Security policy	4.1.1. The moneylender should set up and implement a data protection and security policy that appropriately address relevant data protection obligations based on organisation's operations and business needs. The moneylender may refer to the Data Protection and Security Policy template as a reference. (https://go.gov.sg/dpsecurity-policy).
	4.1.2. As business and IT environments, as well as the cyber threat landscape, tend to evolve over time, the policy should be regularly reviewed to ensure that they are up to date considering the emerging threats, and processes should at least be internally audited to ensure that they align with the policy.
4.2. Develop and implement practices and guidelines on how your hardware and software assets are managed securely	The moneylender should replace hardware and software assets that are unauthorised or have reached their respective End of Support (EOS). In particular, cover the following: (a) Assess risks and obtain management approval for continued use of EOS assets, with ongoing monitoring until replacement. (b) Implement authorisation process for new hardware/software onboarding through management approval, trusted sources verification, and asset listing. (c) Record approval dates in asset inventory after obtaining proper dispensation. (d) Remove all software and hardware without documented approval dates. (e) Securely erase all confidential information before hardware disposal through encryption and reformatting. The moneylender may refer to the Data Protection and Security Policy template (Clause 4.2.2 - Asset Management) as a reference (https://go.gov.sg/dpsecurity-policy).

5. Regular review	
5. Conduct regular review	5.1.1. The moneylender should perform regular IT system audit to be satisfied that its policies and processes are updated and effective in addressing the emerging technology risks, and this includes instances where IT services are outsourced to IT vendors.
	5.1.2. The moneylender should carry out review to ensure latest software updates and patches are installed on devices and systems to address newly discovered security vulnerabilities.
	5.1.3. The moneylender should carry out review and update the following at least annually, or whenever there is any change to the data captured by the organisation: (a) Data protection and security policies (b) Assets inventory lists, including hardware, software and data (c) Configuration settings for hardware and software (d) User account inventory list to ensure all accounts are active and the rights assigned are necessary (e) Data breach management and Incident response plan
	5.1.4. The moneylender should conduct training on cybersecurity and data protection for all employees annually.
	5.1.5. The moneylender should conduct phishing simulation exercises regularly to train the employees to be alert to and protected from Phishing.
	5.1.6. The moneylender should conduct table-top exercise regularly to test the cyber and data breach response plan. The moneylender may download the CSA Incident Response Playbook: (https://www.csa.gov.sg/Tips-Resource/Resources/singcert/incident-responseplaybooks).