**Data Protection Essentials (DPE) Checklist**

# SECTION 1: DPE (ONE-TIME SETUP)

|  |  |  |
| --- | --- | --- |
| **Scope of Service (Data Protection)** | | **Resources / References** |
| **ACCOUNTABILITY** | | | |
| * Registration of the DPO on ACRA BizFile+ and make available the business contact information of DPO to the public * Develop a Data Protection and Security policy * Document data assets and flows using Asset Inventory Map | Yes  No  Yes  No  Yes  No | 1. For ACRA-registered entitities, organisations may register in ACRA BizFile+ ([www.bizfile.gov.sg](https://www.bizfile.gov.sg)).   For non ACRA-registered entities, organisations may register the DPO with PDPC ([www.pdpc.gov.sg/dpo-registration](https://www.pdpc.gov.sg/dpo-registration)).  Refer to the Guide to Register DPO on ACRA BizFile+     1. Data Protection and Security Policy      1. Refer to Annex B in the Data Protection and Security Policy on asset inventory map |
| **TRAINING** | | | |
| * Mandate the staff to complete the PDPA E-learning * Identify and facilitate key personnel to attend PDPC courses (e.g. Fundamentals of the PDPA 2020) | Yes  No  Yes  No | 1. Refer to the [PDPA E-Learning Programme](https://www.pdpc.gov.sg/Help-and-Resources/2018/01/E-Learning-Programme) for all staff. 2. The PDPC courses are: 3. [Fundamentals of Personal Data Protection Act 2020](http://www.pdpc.gov.sg/fundamentals-of-pdpa) 4. [**Optional**] [Practitioner Certificate in Personal Data Protection 2020](http://www.pdpc.gov.sg/practitioner-certificate) |
| **BASIC DATA SECURITY PRACTICES** | | | |
| * Secure configuration of SAAS productivity suite (M365 or Google Workspace) based on CIS benchmark Level 1 * Implement the following security configuration:   + Enable MFA   + Disable auto email forwarding feature * Configure data encryption at rest (including backup data) for all the followings:   + Disk encryption (e.g. Bitlocker)   + Database encryption (e.g. Using customer’s database’s native encryption features) * Configure for data encryption in transit for all the followings:   + secure server administration channel (SSH)   + secure file transmission (e.g. VeraCrypt, 7zip, GNUPG) | Yes  No  Yes  No  Yes  No    Yes  No |  |

|  |  |  |
| --- | --- | --- |
| **Scope of Service (Cybersecurity)** | | **Resources / References** |
| **ASSET** | |  |
| * Provide cybersecurity awareness training for employees in the organisation[[1]](#footnote-1), minimally covering these topics   + Protect yourself from phishing   + Set strong passphrase and protect them   + Protect your corporate and/or personal devices (used for work)   + Report cyber incidents   + Handle and disclose business-critical data carefully   + Work onsite and telecommute in a secure manner * Support the organisation to develop cyber hygiene practices and guidelines for employees to adopt in their day-to-day operations | Yes  No  Yes  No | 1. Agenda of training topics[[2]](#footnote-2) 2. Refer to the Cyber Essentials Self-Assessment Questionnaire |
| * Support the organisation to create and/or maintain an up-to-date asset inventory of the hardware and software assets in the organisation * Support the organisation to develop and implement practices and guidelines on how hardware and software assets are managed securely, including   + Authorisation process to onboard new hardware and software   + Treatment of unauthorized and End of Support (EOS) assets   + Secure deletion and disposal of assets | Yes  No  Yes  No | 1. System and network diagram of organisation setup 2. Refer to Annex B in the Data Protection and Security policy on asset inventory of hardware and software assets 3. Refer to Section 4.2.2 in the Data Protection and Security policy on Asset Management |
| * Support the organisation to create and/or maintain an inventory of sensitive or business-critical data in the organisation * Support the organisation to develop and implement practices and guidelines on how data is managed securely, including   + Protection of data   + Prevention of leakage of data by employees   + Secure disposal of data | Yes  No  Yes  No | 1. Refer to Annex B in the Data Protection and Security policy on asset inventory of business-critical data 2. Refer to Section 4.2.5 in the Data Protection and Security policy on Data Management |
| **SECURE / PROTECT** | |  |
| Anti-Virus/Malware Protection   * Support the organisation with the configuration[[3]](#footnote-3) of anti-malware solutions in the organisation:   + Enable virus and malware scans   + Enable auto update or configure anti-malware solution to update signature files to detect new malware   + Configure anti-malware solution to automatically scan files * Support the organization to review that only fully supported browsers and email client with security controls are in used * Support the organisation with the configuration[[4]](#footnote-4) of firewall solutions in the organisation[[5]](#footnote-5) | Yes  No  Yes  No  Yes  No |  |
| * Support the organisation so that its employees are aware of taking protective steps against malware | Yes  No | N/A – Covered under Cybersecurity Awareness Training |
| Access Control   * Support the organisation to create and/or maintain an up-to-date inventory of accounts in the organisation * Support the organisation to develop and implement the practices and guidelines on the secure management of accounts, including * Management of access of accounts to employees and third parties/contractors, including disabling, removing and locking accounts * Usage of administrator accounts * Support the organisation to develop and implement practices and guidelines on the secure management of physical access to assets * Support the organisation to develop and implement practices and guidelines on secure user authentication, e.g. secure passphrases | Yes  No  Yes  No  Yes  No  Yes  No | 1. Refer to Annex F in the Data Protection and Security policy on Account Inventory 2. Refer to Section 4.2.1 in the Data Protection and Security policy on Access Control 3. Refer to Annex E in the Data Protection and Security policy on Non-Disclosure Agreement 4. Refer to Section 4.2.7 in the Data Protection and Security policy on Passphrase |
| Secure Configuration   * Support the organisation to develop and implement secure configuration for hardware and software assets, including   + Enforcing security configurations or enabling security features for assets and avoiding or updating weak configuration   + Replacing or upgrading insecure configurations and weak protocols   + Turning off features/services that are not used | Yes  No | Refer to Section 4.2.4 in the Data Protection and Security policy on Configuration Management |
| **UPDATE** | |  |
| Software Updates   * Support the organisation to develop and implement practices and guidelines on critical software updates | Yes  No | Refer to Section 4.2.8 in the Data Protection and Security policy on Software Patch Management |
| **BACKUP** | |  |
| Data Backup   * Support the organisation to develop and implement practices and guidelines on backups, including   + Performing backups regularly, depending on business-criticality of data   + Protection of backups   + Storing of critical backups offline | Yes  No | Refer to Section 4.2.3 in the Data Protection and Security policy on Data Backup |
| **RESPONSE** | |  |
| Incident Response   * Support the organisation to develop and implement practices and guidelines on incident response | Yes  No | Refer to Annex G in the Data Protection and Security policy for the incident response plan |

# SECTION 2: DPE (ONE-TIME REVIEW)

|  |  |  |
| --- | --- | --- |
| **REVIEW (6 MONTHS AFTER DP ESSENTIALS IMPLEMENTATION)** | |  |
|  | |  |
| * Latest software updates installed on devices and systems. * Carry out review and update of:   i) Data protection and security policies  ii) Configuration settings for hardware and software  iii) User accounts to ensure all accounts are active and the rights assigned are necessary  iv) Incident response plan   * Refresher on cyber and data protection awareness training for key employees on handling personal data. * Conduct phishing simulation exercises to train the employees to be alert. * Conduct table-top exercise to test the cyber and data breach response plan. * Audit on sharing of passwords such as admin credentials, displaying post-it notes of password publicly or storing passwords in public web folders. * Regular backups according to the backup policy. Backup media regularly tested to ensure that the backup data can be recovered and restored. | Yes  No  Yes  No  Yes  No  Yes  No  Yes  No  Yes  No  Yes  No |  |

1. Modality of training: Delivered online [↑](#footnote-ref-1)
2. Please refer to [CSA Cybersecurity Toolkits for Employees](https://www.csa.gov.sg/employee-toolkit) [↑](#footnote-ref-2)
3. If the organisation is already using an existing solution, the DPE provider is not expected to provide the solution, but support the organisation in reviewing its use and configuration in the organisation. [↑](#footnote-ref-3)
4. If the organisation is already using an existing solution, the DPE provider is not expected to provide the solution, but support the organisation in reviewing its use and configuration in the organisation. [↑](#footnote-ref-4)
5. Network perimeter firewall for organisations with enterprise network setup, and host-based firewall on devices for organisations without enterprise network setup [↑](#footnote-ref-5)