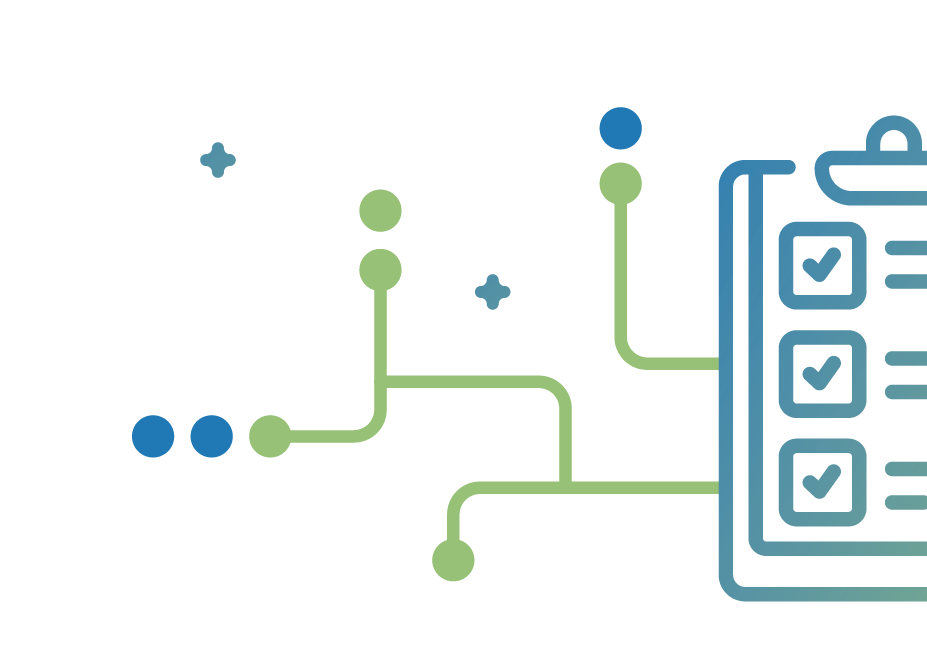


**Applying Data Protection Practices to Guard   
Against Common Types of Data Breaches**

To help organisations perform a review of whether policies, technology controls and processes applicable to their business operations have been put in place to avoid the common gaps that often result in data breaches[[1]](#footnote-1), we have compiled the key relevant data protection practices from the PDPC’s [Guide to Data Protection Practices for ICT Systems](http://www.pdpc.gov.sg/dp-ict) into the following checklists.

Organisations should still refer to the Guide to Data Protection Practices for ICT Systems for implementation of baseline ICT data protection practices within their organisation.



## 

## CHECKLIST 1

## Application security in development and support phase

**OBJECTIVES**

This checklist aims to help organisations put in place good practices during their application development phase and support process, to prevent **coding issues** that could result in application errors leading to the subsequent disclosure of personal data. It will also enhance security awareness and responsibilities during coding.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Policy / Risk Management** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| a. | Develop a Software Development Methodology (“**SDM**”) and perform periodic review for any gaps. |  |  |  |  |  |
| b. | Develop an IT Change Management Process and perform periodic review for any gaps. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| a. | Conduct code review and rigorous unit testing which includes complete testing of functional requirements to verify the compliance to the requirements specs at early stage in system development lifecycle. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| b. | Ensure adequate controls such as fail-safe processing in coding under “if-then-else” exception conditions are in place to prevent improper error handling that may result in leakage of sensitive personal data. |  |  |  |  |  |
| c. | Conduct regression testing and system integration testing which includes complete testing of both functional and non-functional requirements as well as to verify the integration of the interfaces to all its external systems in the middle stage of the system development lifecycle. |  |  |  |  |  |
| d. | Conduct user acceptance testing (“**UAT**”), load testing and stress testing at near-end stage of the system development lifecycle to ensure robustness and security of system. Ensure that the business requirements are properly captured and documented during requirements gathering as these requirements will become the business logic in use case scenarios. It is important that the use case scenarios, performed and validated in the UAT, should be properly planned to simulate real-world usage and it should be as comprehensive as possible. The UAT coverage should also include foreseeable exception handling scenarios, especially when personal data are being transmitted or displayed in these “live” scenarios. |  |  |  |  |  |
| e. | Automate build and deployment processes to minimise manual steps and hence reduce human errors. For example, executing predefined scripts instead of manually typing out commands each time a new build of an application is required; this eliminates errors in typing and the possibility of accidentally leaving out certain commands, as well as deploying the new build to the wrong environment, such as deploying a test build to the production environment. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SOP/IT Operations** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| a. | Do not use or store production data that contains personal data in non-production[[2]](#footnote-2) environments for testing or other purposes. Do not use production data for user acceptance tests. Organisation may consider creating synthetic data from production data using anonymisation techniques[[3]](#footnote-3), or synthetic data generator software. |  |  |  |  |  |
| b. | Perform thorough impact analysis of any software or code changes and design before coding. This provides an accurate understanding of the implications of the proposed changes, which helps to make informed business decision about the areas of the system that may be affected due to the change in the features of the applications. |  |  |  |  |  |
| c. | Document all software functional and technical specifications (e.g. program specifications, system specifications, database specifications). The presence of reliable documentation helps to keep track of all aspects of an application and improves the quality of a software product. |  |  |  |  |  |
| d. | Ensure passwords are not exposed in code or configuration files. State clearly in the ICT policy and ensure that the team or vendors are aware. Scan for such risks during security reviews. |  |  |  |  |  |
| e. | Periodically conduct web application vulnerability scanning and assessments in post deployment. |  |  |  |  |  |

## 

## CHECKLIST 2

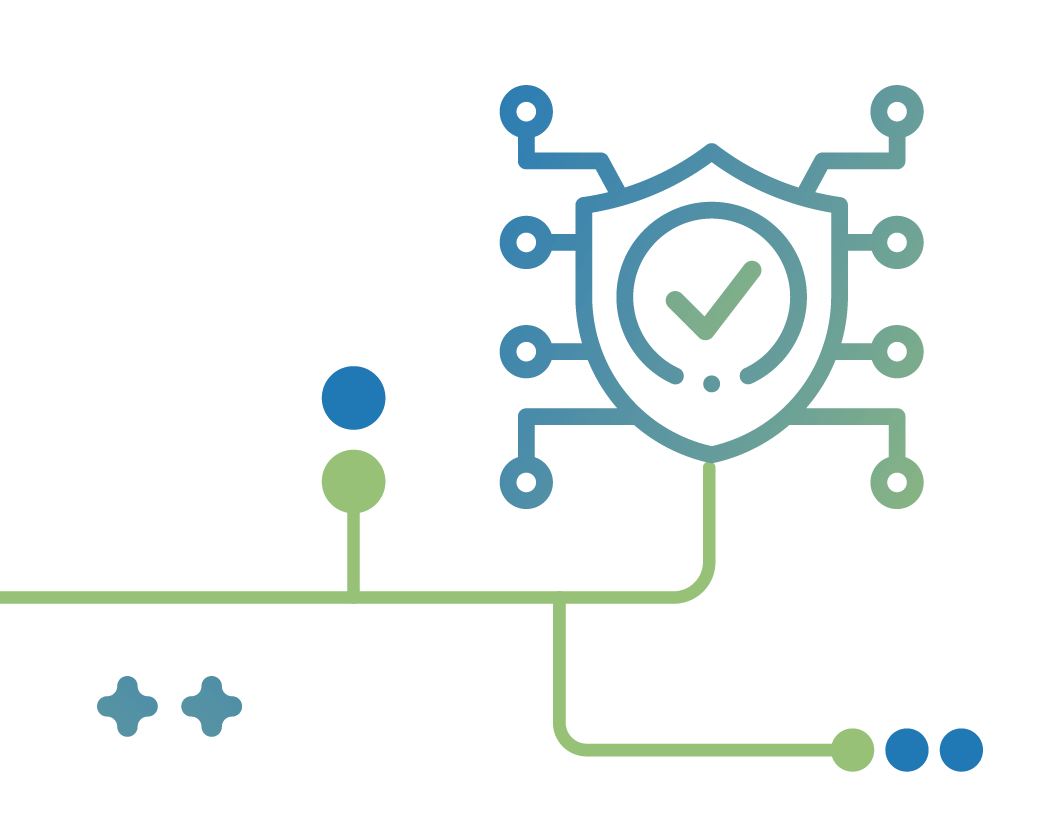
## Infrastructure and system security in ICT systems

**OBJECTIVE**

This checklist aims to help organisations review relevant data protection practices in relation to **configuration management, protection against malware/phishing, enhancing security awareness/responsibilities and strengthening account password management**.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Policy / Risk Management** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| a. | Develop an ICT policy that covers the critical aspects in IT security such as account and access control, password, email, IT risk management, asset and configuration, backup and recovery, hardening and patching |  |  |  |  |  |
| b. | Periodically review and update ICT security policies, standards and procedures to ensure continued relevance, adequacy and effectiveness. This will provide assurance that the data protection practices are kept updated with regulatory and technological developments. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Policy / Risk Management** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| c. | Communicate ICT security policies to both internal stakeholders (e.g. staff), and external parties (e.g. customers). This provides assurance to external stakeholders that their personal data are adequately protected; and provides clarity to internal stakeholders on their responsibilities and security processes on handling personal data in their day-to-day work and business activities. |  |  |  |  |  |
| d. | Identify and empower the person(s) accountable for personal data protection within the organisation, who can effectively direct and oversee data protection initiatives. |  |  |  |  |  |



|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| **Authentication, authorisation and password** | | | | | | |
| a. | Implement access control at the application level to restrict the access to data to a  user role |  |  |  |  |  |
| b. | Define user access control privileges for user roles/rights to data. As a guide, users should not be able to see information that they do not need to know. This should be consistent with the organisation’s access control policy. |  |  |  |  |  |
| c. | Enforce password controls such as requiring a change of password upon first login, minimum password length, restricting use of previous passwords, mandating minimum level of password complexity as well as passwords that expire periodically. |  |  |  |  |  |
| d. | Enforce regular change of passwords. However, the periodic change of passwords can be set longer (i.e. twice a year or once a year) to balance the reasonable efforts that have been put in to enforce minimum level of password complexity (i.e. minimum 12 alphanumeric characters with a mix of uppercase, lowercase, numeric, special char and use of commonly used phrases or paraphrase[[4]](#footnote-4)). |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | | | **Action Plan** | |
| Comply | Partial Comply | Not comply | | Not Applicable | |
| **Web applications and website security** | | | | | | | | | | |
| e. | | Scan uploaded files for malware and perform follow-up action upon detection of malware. Restrict uploads to certain whitelisted file types that the organisation has in use as whitelisted files types may vary from one organisation to another organisation. |  |  | |  | |  | |  |
| f. | | Ensure that files containing personal data are not accidentally made available on a website or through a web application. For example, avoid storing personal data in public folders or disable directory browsing to prevent hackers from finding those files. Enable periodic scan for presence of public folders on the website, conduct periodic reviews of public folder contents. Apply automatic purging of contents within a public folder after a pre-defined retention period. |  |  | |  | |  | |  |
| g. | | Apply secure connection technologies or protocols (e.g. TLS) to websites and web applications that handle personal data. For example, using HTTPS instead of HTTP. |  |  | |  | |  | |  |
| h. | | Perform web application scanning and source code analysis to help detect web vulnerabilities. Vulnerabilities to look out for could include those in the Open Web Application Security Project (OWASP)[[5]](#footnote-5) “Top Ten” list or similar. |  |  | |  | |  | |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **Computer networks** | | | | | | |
| i. | Install endpoint security solutions as defence against malware and maintain up-to-date defence software such as web-proxies, anti-virus/anti-malware and anti-spyware solutions on the servers to protect your computer network against malicious attacks. Specify follow-up action upon detection of malware. |  |  |  |  |  |
| j. | Equip networks with defence devices such as firewalls to protect your computer network connected to the Internet. |  |  |  |  |  |
| k. | Monitor, encrypt and restrict communications between environments to only authenticated and authorised connections, as justified by the nature of the work. |  |  |  |  |  |
| l. | Assess the need for remote access to servers such as configuring remote desktop protocol (“**RDP**”) to be open in the organisation’s network and exposed to the internet. Consider applying additional controls where possible, such as restricting access to specified external IP addresses and ensuring remote desktop is used behind a secure virtual private network (“**VPN**”). |  |  |  |  |  |
| **ICT security and testing** | | | | | | |
| m. | Encrypt exported data and communicate the password separately to the target recipient of the exported data (i.e. internal or external party). |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **ENHANCED PRACTICES** | | | | | | |
| **Authentication, authorisation and password** | | | | | | |
| a. | Use one-time password (“**OTP**”) or two-factor authentication (“**2FA**”)/multi-factor authentication (“**MFA**”) for admin access to sensitive personal data records or large volumes of personal data. |  |  |  |  |  |
| b. | Implement segregation of duties where system tasks are separated and performed by different groups. It is also desirable to have job rotation and cross training for security admin roles and functions. |  |  |  |  |  |
| c. | Limit number of failed logins to minimise brute force attacks. |  |  |  |  |  |
| **Web applications and website security** | | | | | | |
| d. | 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. |  |  |  |  |  |
| **ICT security and testing** | | | | | | |
| e. | Conduct network penetration testing prior to the commissioning of any new ICT system to detect and resolve any vulnerabilities before the system goes ‘live’. |  |  |  |  |  |
| f. | Monitor data export activities to detect data exfiltration and consider configuring a threshold for allowable data export. |  |  |  |  |  |

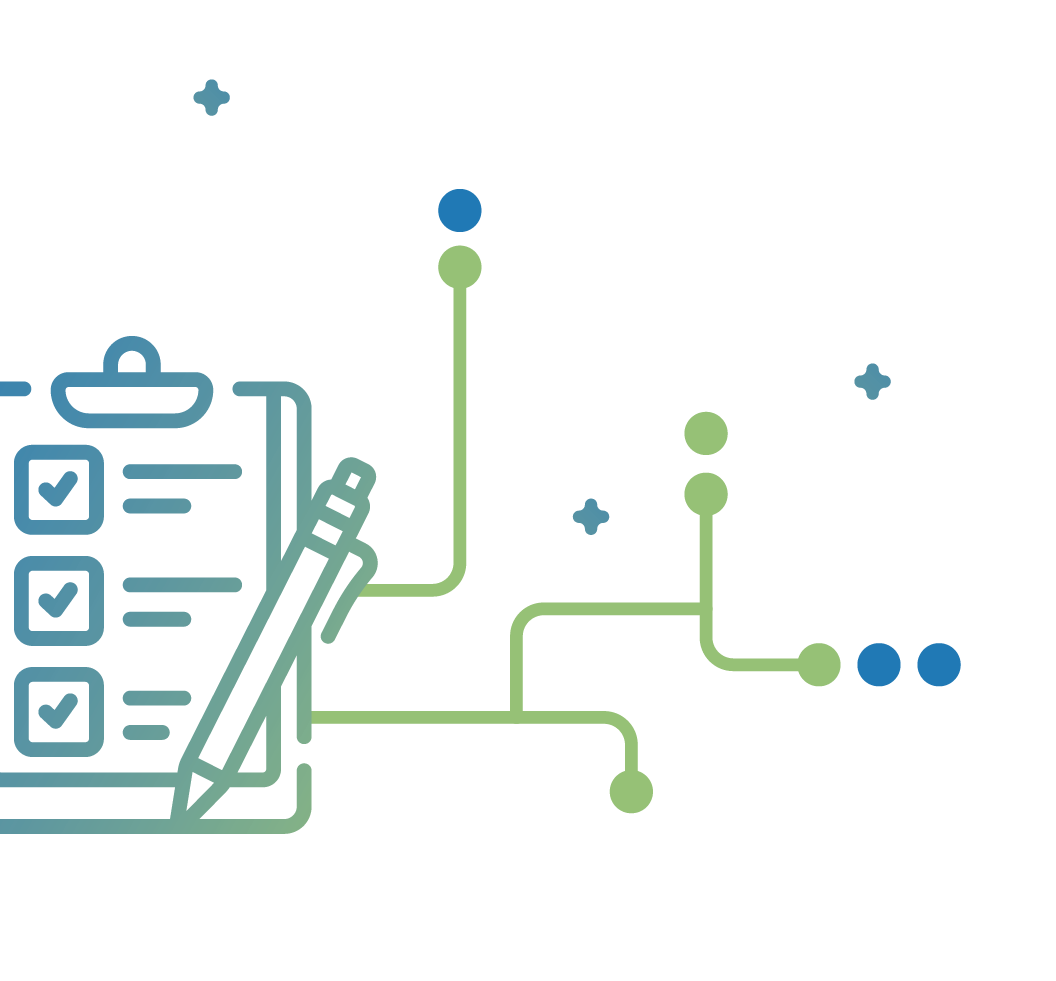
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **ICT Controls** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **Computer networks** | | | | | | |
| g. | Implement intrusion prevention systems (“**IPS**”) solutions which is a device or software application that monitors network or system activities and prevents malicious activities or policy violations. |  |  |  |  |  |
| h. | Implement intrusion detection systems (“**IDS**”) which is a network security appliance that monitors network and system activities for malicious activities and may raise alerts upon detecting unusual activities. |  |  |  |  |  |
| i. | Install security devices that prevent the unauthorised transfer of data out from a computer or network. |  |  |  |  |  |
| j. | Use 2FA and strong encryption for remote access. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure. |  |  |  |  |  |
| k. | Use network proxies to restrict employee access to known malicious websites. |  |  |  |  |  |
| l. | Design and implement the internal network with multi-tier or network zones, segregating the internal network according to function, physical location, access type etc. |  |  |  |  |  |
| **Database security** | | | | | | |
| m. | Encrypt datasets containing sensitive personal data that has a higher risk of adversely affecting the individual should it be compromised or consider database repositories encryption. Review the method of encryption (e.g. algorithm and key length) periodically to ensure that it is recognised by the industry as relevant and secure. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SOP/IT Operations** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **BASIC PRACTICES** | | | | | | |
| **Security awareness** | | | | | | |
| a. | Educate employees on the organisation’s ICT security policies, controls, and procedures for protection of personal data through various training programmes (i.e. courses or online videos). |  |  |  |  |  |
| b. | Keep ICT security awareness training for employees updated and conduct such training regularly. Put in place processes to monitor the awareness level of employees. |  |  |  |  |  |
| c. | Regularly remind the employees to be alert to phishing and other forms of social engineering. Conduct phishing simulation exercises to train your employees to be alert. |  |  |  |  |  |
| d. | Develop personal accountability for individual employee’s actions and responsibilities towards securing or protecting personal data belonging to the organisation or external parties such as encrypting personal data with password before sending via email to an external party. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SOP/IT Operations** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **Compliance, monitoring, alerts, test and audits** | | | | | | |
| e. | Conduct regular ICT monitoring, alerts, security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards. |  |  |  |  |  |
| f. | Apply prompt remedial actions (i.e. system patching, security scans and checking of log files for anomalies) to detect and fix security vulnerabilities and any non-compliance with established policies and procedures. |  |  |  |  |  |
| g. | Maintain audit logs to record the events as logs are important for determining the cause of security incidents and monitoring the overall health of ICT systems. |  |  |  |  |  |
| h. | Implement measures to ensure ICT system logs are reviewed regularly for security violations and possible breaches. |  |  |  |  |  |
| **Authentication, authorisation and password** | | | | | | |
| i. | Regular review of user accounts to ensure all the accounts are active and the rights assigned are necessary (i.e. remove user accounts when a user has left the organisation or update the user’s rights when he/she has changed his/her role within the organisation). |  |  |  |  |  |
| j. | Enforce prohibition on the sharing of passwords such as admin credentials, displaying post-it notes of password publicly or storing passwords in public web folders (including GitHub). |  |  |  |  |  |
| k. | Log successful and failed logins in order to assist detection or investigation into hacking attempts. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SOP/IT Operations** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **ICT security and testing** | | | | | | |
| l. | Ensure personal data in your organisation’s possession are regularly backed up according to the backup policy. Backup media should be regularly tested to ensure that the backup data can be recovered and restored in time to help the business recover from any unplanned event such as data corruption or malicious attack (i.e. virus or malware). |  |  |  |  |  |
| **Computer networks** | | | | | | |
| m. | Document configuration settings and review /test these regularly to ensure they correspond to current requirements such as allowed services, protocols, ports and compensating controls. |  |  |  |  |  |
| n. | Ensure the firewall ports are closed by default and open them when necessary for operational purposes. Conduct periodic review of firewall rules to restrict connectivity to only authorised/ whitelisted servers/IP address and close all unused ports. |  |  |  |  |  |
| o. | Configure web servers securely such as turn off services that are not in use (i.e. disable directory listing, disable banner display, disable/block all unnecessary listener services, turn off unused modules & open ports, avoid using default port numbers/ranges, restrict access to specified external IP ranges). |  |  |  |  |  |
| p. | Maintain a list of whitelisted connections to allow connections to only specific, trusted hosts. |  |  |  |  |  |
| q. | Log and review all RDP login attempts. |  |  |  |  |  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **SOP/IT Operations** | | **Practice Met** | | | | **Action Plan** |
| Comply | Partial Comply | Not comply | Not Applicable |
| **ENHANCED PRACTICES** | | | | | | |
| **Authentication, authorisation and password** | | | | | | |
| a. | Log access to sensitive personal data. |  |  |  |  |  |
| **Computer Networks** | | | | | | |
| b. | Monitor LAN/Wi-Fi regularly and remove unauthorised clients and Wi-Fi access points. |  |  |  |  |  |



BROUGHT TO YOU BY



Copyright 2021 – Personal Data Protection Commission Singapore (PDPC)

The contents herein are not intended to be an authoritative statement of the law or a substitute for legal or other professional advice. The PDPC and its members, officers, employees and delegates shall not be responsible for any inaccuracy, error or omission in this publication or liable for any damage or loss of any kind as a result of any use of or reliance on this publication.

The contents of this publication are protected by copyright, trademark or other forms of proprietary rights may not be reproduced, republished or transmitted in any form or by any means, in whole or in part, without written permission.

1. Refer to PDPC’s handbook on “[How to Guard Against Common Types of Data Breaches](https://www.pdpc.gov.sg/Help-and-Resources/2021/05/Guard-Against-Common-Data-Breaches)” [↑](#footnote-ref-1)
2. Non-production environments include a network, operating system or other systems that are used as a development area or test bed for new software or technologies. [↑](#footnote-ref-2)
3. Refer to PDPC’s “[Guide to Basic Data Anonymisation Techniques](https://www.pdpc.gov.sg/help-and-resources/2018/01/guide-to-basic-data-anonymisation-techniques)” [↑](#footnote-ref-3)
4. A commonly used phrase or paraphrase created by user will help them to remember their own password more easily. If combined with uppercase, lowercase, numbers and special characters, it makes the password stronger and harder to decode. An example is “Learn2bike@5” or “LetsGo2gym@7”. [↑](#footnote-ref-4)
5. Refer to OWASP’s [website](https://owasp.org/). [↑](#footnote-ref-5)