GUIDE TO

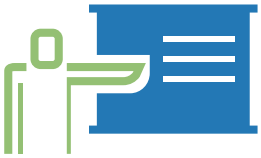
DATA PROTECTION PRACTICES FOR ICT SYSTEMS

SG:DIGITAL

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

CONTENTS

INTRODUCTION



INTRODUCTION

In the face of increasing risk of data protection and cyber threats, organisations need to strengthen their data protection measures and controls for robust and resilient infocomm technology ("**ICT**") systems.

This guide is a compilation of data protection practices from past Advisory Guidelines and Guides released by the Personal Data Protection Commission ("**PDPC**"), and it also incorporates lessons learnt from past data breach cases that should be adopted by organisations in their ICT policies, systems and processes to safeguard the personal data under their care.

The guide has been re-organised in a way that is helpful to any ICT personnel to make reference to (i) policies and risk management practices; (ii) ICT control measures; as well as (iii) Standard Operating Procedures ("**SOPs**") and ICT operations, for each stage of the data lifecycle.

The controls and guidance in this guide are not exhaustive, and not all of them may be applicable with respect to an organisation's business and operation. Effective use of this guide will enable an organisation to achieve a minimum level of data protection. This guide will continue to be updated and improved to incorporate common gaps from reported data breaches and new practices as technology evolves.

DATA PROTECTION PRACTICES FOR ICT SYSTEMS

The data protection practices for ICT systems are grouped into three main sections and their respective sub-sections as shown below.

Policy/Risk Management for ICT systems

- Governance
- Collection of personal data
- Notification of purpose
- Managing consent
- Access, correction and accuracy of personal data
- Housekeeping of personal data
- Retention of personal data

ICT Controls

- Authentication, authorisation and passwords
- Computer networks
- Database security
- Web applications/ website security
- ICT security and testing

SOP/IT Operations

- Security awareness
- Personal computers and other computing devices
- Portable computing devices and removable storage media
- Compliance, monitoring, alerts, testing and audits
- Cloud computing

Each section recommends the basic and enhanced ICT practices that organisations can put in place to support each stage of the data lifecycle. Basic practices are recommended for organisations that handle personal data (e.g. names and email addresses) for generic communication purposes such as direct marketing or customer support.

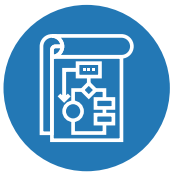
For organisations that hold large quantities of different types of personal data or data that might be more sensitive[1] to the individuals or the organisations, they should additionally implement the relevant enhanced practices suggested in each section. The design and implementation of these protection measures should always take into consideration the extent of the sensitivity of the data based on the nature of business and types of services offered.

POLICY AND RISK MANAGEMENT FOR ICT SYSTEMS

Governance

Good governance enables your organisation to control and direct the approach and resources to mitigate data breach risks throughout the data lifecycle. In doing so, organisations should consider the following four key components of governance:

Clear accountability



Standards,[2] policies and procedures

Risk management

Classification and tracking

[1] *These personal data could include:*
- *Personal data used for transactional or authentication purposes, e.g. credit card info;*
- *Personal data that may result in adverse impact to individuals if disclosed, e.g. health-related data or financial-related data;*
- *Any other data that might result in adverse impact to the organisation if disclosed, e.g. data related to its intellectual property or client base.*

[2] *Standards refer to a set of reliable and common standards in the information technology industry, such as ISO standards or other relevant international standards.*

Governance	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
i. Clear accountability						
a. The senior management of an organisation should provide clear direction on ICT security goals and policies for personal data protection within the organisation. The involvement and support of an organisation's leadership is important in demonstrating commitment to ICT security for data protection.	●	●	●	●	●	●
b. Data protection risks may be managed through ICT controls. Close collaboration is necessary between data protection and ICT security functions within an organisation. This should be evidenced at appropriate levels of its governance structure.						
ii. Standards, policies and procedures						
c. An organisation is required to develop and implement ICT security policies for data protection. Key ICT policies would include: • Account and access control policy • Backup/retention policy • Password policy The policies will help to provide management with the direction as well as guidance for all ICT system implementations and activities related to data protection in ICT systems in accordance with business objectives and relevant laws and regulations. Specifically, classification of data should not be conducted in the abstract. It is the repository or dataset that should be classified, based on their content. This will then allow management to decide the level of ICT, process or other controls that need to be implemented for the system.	●	●	●	●	●	●
d. 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.						
e. Communicate ICT security policies to both internal stakeholders (e.g. staff) and external parties (e.g. customers).[3] 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 in handling personal data in their day-to-day work and business activities.						

[3] *Refer to the Accountability Obligation under the Personal Data Protection Act (PDPA).*

Governance	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
iii. Risk Management						
f. Institute a risk management framework to identify security threats to repositories or datasets containing personal data, assess the risks involved and determine the controls to mitigate or minimise such risks.	●	●	●	●	●	●
g. Periodically assess the effectiveness of the risk mitigation controls.						
h. Assess and mitigate the security risks involved in outsourcing or engaging external parties for ICT services.						
iv. Classification and tracking						
i. Classify and manage repositories or datasets containing personal data by considering the potential adverse impact (e.g. reputational or financial) to the individuals involved should the data be compromised.	●	●	●	●	●	●
j. Conduct data protection impact assessment ("**DPIA**") before development to assess the types of personal data and the data processing activities required for achieving the purposes of a new ICT system.						
k. Conduct periodic checks for personal data stored in ICT systems. For personal data that is not required in any form anymore, securely dispose of the data. If there is a need to retain the data but in anonymised or aggregated form, e.g. for performing data analytics, consider anonymising the data.				●	●	●
l. Conduct physical asset inventory checks regularly to ensure that all computers and other electronic devices (e.g. portable hard drives, printers, fax machines) used to store or process personal data are accounted for.		●		●		

Collection of personal data

Personal data that are collected but not used will pose unnecessary data protection and cyber threat risks to the organisation. Collection of unnecessary personal data increases the risks and impact of data breaches. Additional resources needed to protect these unnecessary personal data can be avoided by simply not collecting them in the first place. Data minimisation is a good way for organisations to examine what personal data they really need.

Collection of Personal Data	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
i. Minimise collection of personal data						
a. Do not collect personal data unless it will be used and there is valid purpose for doing it. Trace every data element that you are collecting to identify which internal department uses it, how it is used and whether it is necessary.	●					
b. When different types of personal data can be used to achieve the same purpose, collect the least sensitive types of personal data (e.g. collect approximate location data of users rather than their exact locations).	●	●	●			
ii. Collect information on personal identifiers (e.g. national identification number) only when absolutely necessary						
c. Collect NRIC[4] numbers if required under the law or only when necessary to accurately establish or verify the identity of the individual.	●					
d. Restrict collection/storage of NRIC numbers to forms, repositories or datasets that need this information. Use an internal customer or employee ID when an NRIC number is not necessary. This may reduce the classification of the repositories or datasets that do not need NRIC numbers.	●			●		
iii. Be aware of metadata						
e. Personal data may be inadvertently collected in the form of metadata (e.g. EXIF data in image files). Consider not collecting such data or removing them if they are not needed.	●					
iv. Avoid continuous automatic collection of personal data						
f. Collect personal data only when needed, instead of continuously. For example, provide the option for users to allow their geolocation data to be collected only when the app they are using requires such data, rather than to be automatically obtained continuously.	●					

[4] *Refer to PDPC's Advisory Guidelines on the Personal Data Protection Act for NRIC and Other National Identification Numbers.*

Notification of purpose

It is important for organisations to notify individuals of the purposes of and obtain their consent for collecting, using and disclosing their personal data, unless any exception applies. To improve user-friendliness for consumers, notifications provided through ICT systems should be easy to understand, be provided dynamically and adopt a layered approach.

Notification of Purpose	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Maximise your touch points with the consumer and make full use of them to provide "just-in-time" notifications in bite-sized portions that are relevant to the interaction. Avoid lengthy notifications.	●	●	●			
b. Use a "layered notice" to convey the organisation's purposes and policies where appropriate, by providing the most important or basic information prominently (e.g. on the pop-up screen during app installation) and detailed information inside the privacy policy or other parts of your website.						
c. When sending notifications to the targeted audience, choose the most appropriate channel(s) or approach (e.g. in writing through a form, on a website, infographics or orally in person) which best suits the context of the business.	●		●			

Managing consent

Consent can be obtained in a few different ways. As a good practice, an organisation should obtain consent in writing or recorded in a manner that is accessible for future reference. This will be useful if, for example, the organisation is required to prove that it had obtained consent. Organisations can also consider managing different versions of consent effectively and easily via an ICT system to check against the consent records of the individuals.

Managing Consent	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. When capturing consent, ensure that the user has performed an explicit action to indicate consent, e.g. the user needs to tick a checkbox and the checkbox should not be pre-ticked (i.e. automatically selected by default).	●	●	●			
b. Ask separately for consent to receive marketing materials. For example, if the user will be asked for consent to receive marketing materials, ask for it separately from the consent to collect personal data, e.g. via a second checkbox.						

Managing Consent	Data Lifecycle					
Enhanced Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
c. Keep copies of consent messages, as changes made to the text may result in different versions with different effective dates. Keeping copies allows for easy checking of the exact message used during a certain date and time. Such records can be useful in the event of disputes with users.	●	●	●			
d. Maintain a consent register to keep a record of what users may have consented to and what they have not, and when the consent was obtained. This can be achieved via a consent management system.	●	●	●	●		

Access, correction and accuracy of personal data

To increase consumer trust in the organisation, organisations should always make reasonable efforts to ensure accuracy and completeness of personal data in their possession, especially when the data are likely to be used to make a decision that will affect the individual. Access and correction requests are intended to help ensure accuracy and completeness.

Access, Correction and Accuracy of Personal Data	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Identify data that is often used and relied on, and periodically remind users to view their personal data details and verify that they are correct. For example, this could be done in pop-up windows in apps.	●	●	●			
Enhanced Practices						
b. Provide users with a self-management facility to allow them to self-help and manage their own personal data. This minimises the possibility of human error as well as reduces employee effort and time.	●	●	●			

Housekeeping of personal data

Organisations usually focus on protecting their main source of personal data (e.g. their database) but may neglect to protect secondary storage locations of personal data, which are often temporary or one-time in nature. These include files that have been created for an ad hoc purpose which are often not stored in central repositories but on user devices or random network drives. Hence, housekeeping is especially relevant to these secondary sources which are often forgotten and may result in a data breach.

Housekeeping of Personal Data	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Protect temporary files such as interface files or data migration files while they exist and remove them once they are not required.		●	●	●		●
b. Implement a routine schedule to identify and remove temporary files when these are no longer needed.	●	●	●	●		

Retention of personal data

The organisation should cease to retain personal data in their ICT systems once the purpose for which the personal data was collected no longer exists. Keeping the personal data for long periods increases the cybersecurity risks to the organisation. A good way to minimise these risks is for the organisation to assess whether the retention of personal data may be necessary based on its business needs or legal purposes.

Retention of Personal Data	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Have an appropriate personal data retention policy which sets out the varying minimum/maximum retention periods for repositories/ICT systems containing personal data. ICT controls could be implemented in ICT systems to enforce retention periods, especially for organisations that hold a large quantity of personal data.				●	●	●
b. Where there is a need to keep the data beyond the retention period, review and anonymise records[5] to prevent re-identification to an individual.				●	●	
c. Delete records that are no longer needed. The organisation may implement ICT systems to flag records which have reached the end of the retention period.				●	●	●
d. Perform physical disposal of hard disks or other known methods of destruction of storage media, such as degaussing and incinerating, when secure deletion, erasure or deletion of personal data stored on the electronic media is not possible. This may be the case with faulty storage media.						●
e. Before redeploying, exchanging or disposing of electronic (re-writable) media, always perform secure deletion, erasure, purging or destruction of electronic personal data on storage media.						

[5] *Refer to PDPC's Guide to Basic Data Anonymisation Techniques.*

ICT CONTROLS

Authentication, authorisation and passwords

Authentication and authorisation processes in ICT systems are commonly used to ensure that information is accessed only by the authorised persons performing the intended activities. It is a good practice to set appropriate access control rules, access rights and restrictions for specific user roles. It is also good to have stronger requirements for administrative accounts, such as complex passwords or 2-Factor Authentication ("**2FA**") /Multi-Factor Authentication ("**MFA**"). Unauthorised access is one of the most common types of data breaches. This can happen, for example, through the use of a weak password which is easily guessed by hackers. Hence, accounts and passwords need to be managed securely.

Authentication, Authorisation and Passwords	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
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 a change of password upon first logon, a minimum password length, restricting reuse of previous passwords, mandating a minimum level of password complexity as well as a maximum validity period of a password.						
d. Enforce regular change of passwords. However, the periodic change of password can be set longer (i.e. twice a year or once a year) to balance the reasonable efforts that have been made to enforce a minimum level of password complexity (e.g. minimum 12 alphanumeric characters[6] with a mix of uppercase, lowercase, numeric, special characters and commonly used phrases or paraphrases[7]).	●	●	●	●	●	
e. Regular review of user accounts to ensure that 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).	●	●		●	●	

[6] *Refer to CSA's Guideline on "How to create a strong password".*

[7] *A commonly used phrase or paraphrase created by the user will help them to remember their own password more easily. When combined with numbers and uppercase, lowercase and special characters, the password becomes stronger and harder to decode. Examples are "Learn2bike@5" or "LetsGo2gym@7".*

Authentication, Authorisation and Passwords	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
f. Have clear policies that prohibit the sharing of passwords such as admin credentials, publicly displaying passwords on Post-it notes or storing passwords in public web folders (including Github).	●	●		●	●	
g. Log successful and failed logins in order to assist detection or investigation into hacking attempts.						
Enhanced Practices						
h. Use a one-time password ("**OTP**") or 2FA/MFA for admin access to sensitive personal data records or large volumes of personal data.						
i. 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.	●	●		●	●	
j. Log access to sensitive personal data.						
k. Limit the number of failed logins to minimise brute force attacks. This can be configured under "account lockout threshold" via group policy at domain level as part of system management.						

Computer networks

Computer networks allow communication between computers and devices that are connected to them. Internal corporate computer networks may be connected to external networks such as the Internet. It is important for an organisation to ensure that its corporate computer networks are secured. Unauthorised and unsecured network connections can lead to a weak defence in the ICT system. Any vulnerabilities in the network may allow cyber attackers to penetrate, which may result in theft or unauthorised use of personal data.

Computer Networks	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Equip networks with defence devices such as firewalls to protect your computer network connected to the Internet.						
b. 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.						
c. Document configuration settings and review/test these regularly to ensure that they correspond to current requirements such as allowed services, protocols, ports and compensating controls.						
d. Monitor, encrypt and restrict communications between environments to only authenticated and authorised connections, as justified by the business.						
e. Ensure that the firewall ports are closed by default and open them when necessary for operational purposes. Conduct periodic reviews of firewall rules to restrict connectivity to only authorised/ whitelisted servers/IP addresses and close all unused ports.	●	●		●	●	
f. Configure web servers securely by turning 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 and open ports, avoid using default port numbers/ ranges, and restrict access to specified external IP ranges).						
g. Maintain a list of whitelisted connections to allow connections to only specific, trusted hosts.						
h. 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**").						
i. Log and review all RDP login attempts.						
Enhanced Practices						
j. Implement an intrusion prevention system ("**IPS**") solution, which is a device or software application that monitors network or system activities and prevents malicious activities or policy violations.	●	●		●	●	
k. Implement an intrusion detection system ("**IDS**"), which is a network security appliance that monitors network and system activities for malicious activities and may raise alerts upon detecting unusual activities.						

Computer Networks	Data Lifecycle					
Enhanced Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
l. Install security devices that prevent the unauthorised transfer of data out from a computer or network.						
m. Monitor LAN/WiFi regularly and remove unauthorised clients and WiFi access points.	●	●		●	●	
n. 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.						
o. Use network proxies to restrict employee access to known malicious websites.	●	●				
p. 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

Databases are used to store and manage data. Some could contain personal data, and organisations need to put in place adequate protection for these databases. Different database products and their various editions tend to have different security features. Organisations should consider their security requirements when selecting a database product. Considerations should include identifying the types of personal data to be stored and the risk of adverse impact to the individual should such data be compromised.

Database Security	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Enforce strict control over users' activities such as limiting their direct access to the database, ability to execute arbitrary SQL commands or access the database schema.						
b. Log all database activities such as any changes to the database and data access activities to track unauthorised activities or anomalies.		●		●	●	
c. Check that the database is secured and not placed in a vulnerable spot within the network. For example, the database should be placed behind a firewall.						

Database Security	Data Lifecycle					
Enhanced Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
d. Consider database repositories encryption or encrypt datasets containing sensitive personal data that have a higher risk of adversely affecting the individual should they be compromised. 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.		●		●	●	
e. Implement tight control over access to personal data based on the sensitivity of the data. For example, the database can be configured to restrict users from viewing data by excluding columns containing sensitive data such as credit card numbers.	●	●		●	●	

Web applications and website security

Websites and web applications are often used to communicate or provide services to customers or the public with activities such as member logins, rewards redemption, event registration and feedback. Organisations that have public-facing websites should take precautions against common threats to websites and web applications, which include malicious file uploads, cross-site scripting ("**XSS**"), SQL injection and URL manipulation. Organisations should thus ensure that the protection of personal data and the security of the website are key design considerations at the start of any project implementation.

Web Applications and Website Security	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Ensure that the system validates all data input by users so that no unexpected inputs can be keyed in through the user interface.	●	●				
b. Scan user uploaded files for malware and perform follow-up action upon detection of malware. Restrict user uploads to certain whitelisted file types that the organisation may have in use, as whitelisted files types may vary from one organisation to another.	●	●		●		
c. Avoid storing personal data in a cookie as a safeguard against hackers reading the contents of the cookies.						
d. Perform cookie data validation, as well as URL validation, to correspond with the session in use to prevent man-in-the-middle attacks.	●	●				

Web Applications and Website Security	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
e. 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 scans for the presence of public folders on the website and conduct periodic reviews of public folder contents. Apply automatic purging of contents within a public folder after a pre-defined retention period.	●	●		●		
f. Do not allow 'backdoors' in the form of 'secret' URLs or debugging logs that allow access to personal data without user authentication. Do not rely on the robots exclusion protocol (robots.txt) to hide webpages.						
g. Apply secure connection technologies or protocols, such as TLS, to websites and web applications that handle personal data. For example, use 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's ("**OWASP**")[8] "Top Ten" list or similar.	●	●				
i. Do not allow multiple sessions for the same user where the use case does not need support for multiple sessions. In the event that multiple sessions are required, the user should be notified of other concurrent sessions that are still logged on.						
Enhanced Practices						
j. Use non-persistent cookies for session management purposes. This forces the session to disappear from the client once the web browser instance is closed. When personal data are stored in cookies, consider very carefully if they are really required. If sensitive data are persisted in the cookie, ensure that the entire cookie is encrypted and stored for the duration it is needed by setting a short expiration time to secure the cookies.	●	●		●		
k. Use a web application firewall ("**WAF**") to defend against typical web application attacks such as SQL injection and XSS attacks. WAFs can act as another layer of security in addition to the application code level.		●				

[8] Refer to OWASP's website.

ICT security and testing

Organisations should always ensure that the protection of the personal data and the security of the ICT system is the key design consideration at each stage of the system development lifecycle. Otherwise, making changes to the system to resolve any security breaches subsequently will incur more cost to the organisation.

Coding issues have been raised as the main cause of a number of data breach incidents that occurred in the recent years. As such, software developers and other ICT personnel should always keep abreast of current and emerging ICT security threats in order to design, test and maintain ICT systems capable of protecting personal data stored.

ICT Security and Testing	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Do not use or store production data that contains personal data in non-production[9] environments for testing or other purposes. Do not use production data for user acceptance tests. Organisations may consider creating synthetic data from production data using anonymisation techniques.[10]	●	●		●		
b. Perform thorough impact analysis of any software or code changes and design (e.g. use of global variables) before coding. This provides an accurate understanding of the implications of the proposed changes, which helps in making informed business decisions about the areas of the system that may be affected due to the change in the features of the applications.						
c. Conduct code review and rigorous unit testing which includes complete testing of functional requirements to verify the compliance with the requirements specifications at the early stage in the system development lifecycle.						
d. Ensure that 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.		●				
e. Conduct regression testing and system integration testing which includes complete testing of both functional and non-functional requirements as well as verifying the integration of the interfaces to all its external systems in the middle stage of the system development lifecycle.						

[9] *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.*

[10] *Refer to Guide to Basic Data Anonymisation Techniques.*

ICT Security and Testing	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
f. Conduct user acceptance testing ("**UAT**"), load testing and stress testing at the near-end stage of the system development lifecycle to ensure robustness and security of the 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, be properly planned to simulate real-world usage and 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.		●				
g. Post deployment, periodically conduct web application vulnerability scanning and assessments.						
h. Document all software functional and technical specifications (e.g. program specifications, system specifications and 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.	●	●		●		
i. Ensure that 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 a malicious attack (virus or malware).						
j. Ensure that passwords are not exposed in code or configuration files. State this clearly in the ICT policy and ensure that the team or vendors are aware. Scan for such risks during security reviews.		●		●		
k. Automate build and deployment processes to minimise manual steps and hence reduce human errors. For example, execute 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 in deploying the new build to the wrong environment, such as deploying a test build to the production environment.						
l. Encrypt exported data and communicate the password separately to the target recipient of the exported data (i.e. internal or external party).		●	●			

ICT Security and Testing	Data Lifecycle					
Enhanced Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
m. Conduct network penetration testing prior to the commissioning of any new ICT system to detect and resolve any vulnerabilities before the system goes 'live'.		●				
h. Monitor data export activities to detect data exfiltration and consider configuring a threshold for allowable data export.		●	●	●		

SOP/IT OPERATIONS

Security awareness

Increasing awareness of ICT security threats and protection measures among employees as well as ensuring that appropriate internal policies and processes are in place helps to reduce the risk of data breaches through system misuse or mistakes. An example of awareness among employees is being cautious about malware phishing or other forms of social engineering. With employees having unrestricted access to the Internet, they should also be made aware of the security policies and standards relevant to their work.

Security Awareness	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
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. Conduct ICT security awareness training to keep employees updated on common topics such as password management, phishing/social engineering protection, corporate/personal device protection, reporting cyber incidents, and conduct such training regularly. Put in place processes to monitor the awareness level of the employees.	●	●	●	●	●	●
c. Conduct regular phishing simulation exercises to remind employees to be alert to phishing emails[11] and other forms of social engineering.	●	●				

[11] *Spot phishing emails that typically have web and email addresses that do not look genuine, are poorly written, have suspicious attachments, request for personal information and demand urgent action.*

Personal computers and other computing devices

Personal computers and other computing devices (collectively referred to here as "computers") are commonly used by employees for communication and other work purposes. These computers are commonly installed with software such as email, word processing, spreadsheet and presentation tools. Often, in the course of work, some amount of personal data may be stored on the computer's local storage, like its hard disk. Therefore, it is important that users take precautions to safeguard their personal data as well as company data assets with some security measures.

Personal Computers and Other Computing Devices	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Protect computers by using password functions. Examples are keying in of a password during boot-up, requiring login to the operating system and locking the screen after a period of inactivity.	●	●		●		
b. Software that is not required for work or other official use should not be installed, especially software that is obsolete and/or unsupported by proper vendors. The less software installed on a computer, the lower the likelihood that vulnerabilities are present.	●	●				
c. Perform regular scans such as anti-virus scans and anti-malware scans on a computer and schedule constant updates to the anti-virus protection software. Software updates help to patch security flaws and protect the documents/personal data on the computer.		●				
d. Prevent unauthorised personnel from easily viewing the screens of personal computers by using privacy filters, or through positioning of the personal computer.	●	●				

Personal Computers and Other Computing Devices	Data Lifecycle					
Enhanced Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
e. Assess various types of data encryption that are available. These include full disk encryption, virtual disk encryption, volume encryption, file/folder encryption and application-level encryption. Encrypting personal data on a computer's local storage provides another layer of protection.						
f. Periodically review the method of encryption (e.g. AES algorithm and a minimum of 128-bits key length) to ensure that it is recognised by the industry as relevant and secure. Typically, the longer the encryption key length, the more secure the encryption. It is also important to manage and protect the encryption keys by keeping them secure and separate from the encrypted data.	●	●		●		
g. Disallow anonymous or guest logins where the computer is deemed to contain confidential documents about company assets or sensitive personal data records.						
h. Disallow non-administrator users from booting up a computer using external or removable storage media.						
i. Disallow non-administrator employees from installing software or changing security settings, except on a need-to basis. Keep administrator accounts for administrator use only.		●		●		

Portable computing devices and removable storage media

Common portable computing devices used in organisations include notebook computers, tablets and mobile phones. Removable storage media such as USB hard disks, backup tapes, USB flash or thumb drives as well as memory cards are also commonly used.

Portable computing devices and removable storage media are generally considered more susceptible to being misplaced or stolen compared to desktop personal computers. Additional security measures, such as encryption, should be taken to protect these devices and media especially if personal data are stored within them. This is to prevent unauthorised disclosure, modification, removal or destruction of personal data stored on these devices and media.

Security measures taken to protect portable computing devices should apply whether the devices are issued by organisations or owned by employees (e.g. Bring Your Own Device or BYOD).

Portable Computing Devices and Removable Storage Media	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Maintain an updated inventory of the portable computing devices and removable storage media that may be used by your organisation to store personal data.				●		
b. Minimise storage of personal data on portable computing devices and removable storage media. Erase personal data that are no longer required as soon as possible.				●		●
c. Secure portable computing devices and removable storage media used to store personal data when not in use (e.g. under lock and key or attaching them to a fixture with a security cable).				●		
Enhanced Practices						
d. Enable remote device locking and wiping features for portable computing devices that contain or are able to access sensitive or large volumes of personal data.		●				

Compliance, monitoring, alerts, test and audits

Regular assurance checks help organisations ensure that ICT security controls developed and configured for the protection of personal data are properly implemented and practised. If, for example, software patches are not updated as recommended by the third-party software provider, then they may not contain the latest cybersecurity updates and therefore may compromise the organisation's defence against cyber attacks.

Strong compliance with the policies and processes as well as implementation of ICT controls are key foundations in combatting cybersecurity issues. Such measures also strengthen the incident response capabilities of an organisation.

Compliance, Monitoring, Alerts, Test and Audits	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Conduct regular ICT monitoring, alerts, security audits, scans and tests to detect vulnerabilities and non-compliance with organisational standards.	●	●	●			
b. Apply prompt remedial action (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.	●	●		●		
c. 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.	●	●				
d. Implement measures to ensure that ICT system logs are reviewed regularly for security violations and possible breaches.						
e. Ensure that outsourced IT vendors are aware that the organisation intends to use their services to handle personal data and they are clear on their responsibilities and requirements for data processing.[12]	●	●	●	●	●	●
f. Understand the features and limitations of the solution (including plug-ins) that is processing personal data before putting it into use. For example, when using WordPress plug-ins, understand the features of the plug-ins by reading online documentation provided and change the necessary configurations from default setting such that data collected in forms are not published in a publicly accessible table.	●	●				
g. Develop a data breach management plan to manage and respond to data breaches more effectively. Such plans should consider the organisation's business processes and needs, and cover the spectrum of the use of data throughout the data lifecycle.[13]	●	●	●	●	●	●

[12] *Refer to PDPC's Guide to Managing Data Intermediaries.*
[13] *Refer to PDPC's Guide on Managing and Notifying Data Breaches under the PDPA and Checklist for Incident Response Management (see Annex).*

Cloud computing

Cloud computing offers agility, efficiency and flexibility for companies of all sizes to consume technology wherever the businesses may be located, and allows improved speed to market. It is seen as one of the growing forces in the global IT landscape.

Organisations should be aware that the design and operations of cloud computing differ to some extent from traditional non-cloud systems. Organisations that adopt cloud services for the management of personal data need to be aware of the security and compliance challenges that are unique to cloud services as well as the implications if data are compromised in a security breach. As such, organisations have to choose a cloud service provider ("**CSP**") with qualified credentials and work closely with them in a shared responsibility model to securely protect the personal data residing in the cloud solution.

Cloud Computing	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
a. Ensure that the CSP is ISO certified for the relevant standards as necessary.[14] Relevant standards may include ISO/IEC 27001:2013,[15] ISO/IEC 27017:2015,[16] ISO/IEC 27018:2019,[17] MTCS SS584[18] or other recognised international standards. Obtain a copy of the certification for your records if possible.						
b. Have a clear understanding of the levels of protection as well as the security measures put in place by the CSP to protect your organisation's personal data on the cloud, and select the relevant settings required by your organisation that will ensure proper protection of the organisation's personal data.	●	●	●	●	●	●
c. Have a clear understanding of the shared responsibility model defined by the CSP for the organisation's selected cloud service model, e.g. IaaS, PaaS and SaaS. Regardless of deployment, the organisation is generally responsible for their own data, endpoints, identity and access management. They should provide additional protection for the parts of the ICT system or personal data that are still under direct control of the organisation.						

[14] *Refer to Guide to Cybersecurity for Law Practices by The Law Society of Singapore.*
[15] *Refer to ISO Standards ISO/IEC 27001:2013.*
[16] *Refer to ISO Standards ISO/IEC 27017:2015.*
[17] *Refer to ISO Standards ISO/IEC 27018:2019.*
[18] *Refer to MTCS SS584 Standards.*

Cloud Computing	Data Lifecycle					
Basic Practices	Collection	Use	Disclosure	Storage	Archival	Disposal
d. Have a clear understanding of the escalation process and the escalation service levels that the CSP is committed to providing in the event of data breach incidents.	●	●	●	●	●	
e. Cloud service providers may receive lawful requests from law enforcement or judicial authorities to provide access to personal data hosted with them. Your contract should at least require the CSP to inform you when they receive such requests, and before disclosing your data, unless doing so is prohibited by law.			●			
f. Negotiate for the CSP's responsibilities by providing clear operational requirements to them (e.g. conduct third-party audits/penetration tests and sharing of such reports/test results) and including these within the contractual agreements.	●	●	●	●	●	●
g. Keep the encryption keys secure and separate from where the encrypted data are. There are several methods to consider: storing encryption keys on premises while personal data are in the cloud or utilising commercial key management solutions from a third-party vendor.		●		●		

CONCLUSION

CONCLUSION

Organisations and their vendors are encouraged to develop good practices in all ICT systems and processes within their businesses to ensure that they are collecting the right data, providing proper transparency for their collection, protecting and processing the data properly and destroying the data once there are no longer business needs for it. Implementing good data protection practices in accordance with the data lifecycle is important in minimising the risk to organisations, their customers and stakeholders.

ANNEX

ANNEX

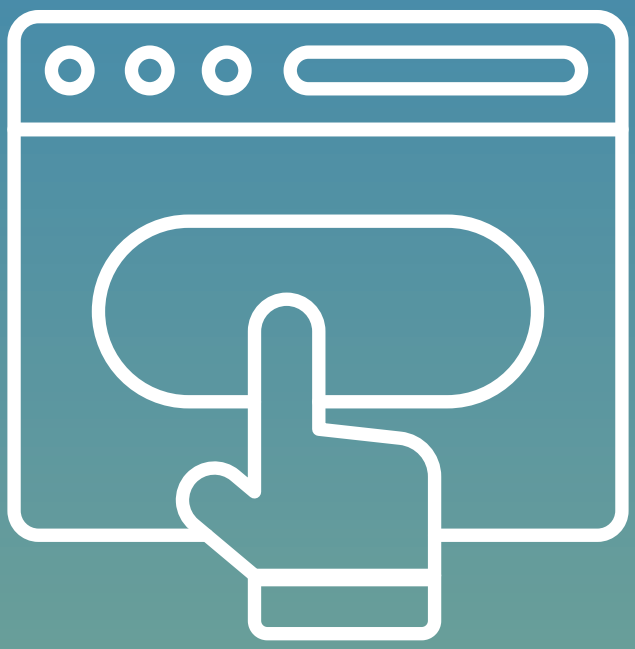
Below is a checklist of good practices that organisations should include in the development of their data breach management plan.

Checklist for Incident Response Management[19]

Good ICT Practices	Practice Met				Action Plan
Basic Practices	Comply	Partial Comply	Not Comply	Not Applicable	
Preparation					
a. Identify key contact information such as designated internal incident response handler, appointed third-party incident response provider, regulatory bodies, law enforcement agencies, SingCERT, etc.					
b. Identify crucial investigation resources such as network diagrams, current baseline of IT systems' activities, backups of important data, etc.					
c. Develop relevant plans such as prevention and detection plans, crisis management and communication plan, business continuity plan, etc.					
d. Identify and understand common types of attacks that could affect your organisation and develop action plans to deal with attacks such as malware, phishing, ransomware, data breaches, etc.					
e. Action plans developed to respond to common incidents are accessible and any updates are communicated to the relevant parties.					
Detection and Analysis					
f. Prepare to handle any incident, in particular those involving common attack vectors such as system misconfigurations, human lapses, internet downloads, etc.					
g. Regularly review and check for possible incident precursors and indicators from internal and external sources such as system and network logs, SingCERT alerts, etc.					
h. Able to make an initial assessment and prioritise the next steps when affected by a cyber incident.					

[19] *This checklist is referenced from CSA's Incident Response Checklist. Please access the full checklist from CSA's website.*

Good ICT Practices	Practice Met				Action Plan
Basic Practices	Comply	Partial Comply	Not Comply	Not Applicable	
Detection and Analysis					
i. The organisation has an SOP for gathering forensic and operational evidence for the purposes of incident resolution and legal proceedings.					
j. Possess knowledge of stakeholders and fiduciary obligations regarding incident reporting when a cyber incident occurs.					
Containment, Eradication & Recovery					
k. Able to develop a containment strategy when responding to a cyber incident that can range from isolating compromised devices to closing vulnerable ports and mail servers.					
l. Understand the need to carry out threat eradication on affected systems before resuming operations, which can take the form of wiping out the malware, disabling breached accounts and patching exploited vulnerabilities.					
m. Understand the steps required to recover affected systems and resume operations, including restoring systems from backups, enforcing password changes, tightening network perimeter security, etc.					
n. Even after a threat has been eliminated, the organisation recognises the need to continue monitoring their network for signs of intrusion and to maintain vigilance.					
Post-Incident Review					
o. After incident resolution, the organisation conducts a post-incident review to identify and resolve deficiencies in the incident response plan, build on lessons learnt and assess if additional security measures are required to strengthen the organisation's security posture.					



ADDITIONAL RESOURCES

ADDITIONAL RESOURCES

Organisations and their vendors are encouraged to refer to the following resources on the PDPC website, which provide more information on the areas that are mentioned briefly in this guide.

Advisory Guidelines

- Chapter 17 of the Advisory Guidelines on Key Concepts under the PDPA (The Protection Obligation)
- Chapter 18 of the Advisory Guidelines on Key Concepts under the PDPA (The Retention Limitation Obligation)
- Chapter 6 of the Advisory Guidelines on the PDPA for Selected Topics (Online Activities)
- Chapter 20 of the Advisory Guidelines on Key Concepts under the PDPA (The Data Breach Notification Obligation)
- Advisory Guidelines on the Personal Data Protection Act for NRIC and other National Identification Numbers

PDPC Resources

- Handbook on How to Guard Against Common Types of Data Breaches
- Guide to Managing Data Intermediaries
- Guide on Managing and Notifying Data Breaches under the PDPA
- Guide to Basic Data Anonymisation Techniques
- The Accountability Obligation under the PDPA

Other Resources

- SS ISO/IEC 27001 & 27002 and MTCS SS584 standards can be found on the Singapore Standards Council website
- Guide to Cybersecurity for Law Practices

#SGDIGITAL

Singapore Digital (SG:D) gives Singapore's digitalisation efforts a face, identifying our digital programmes and initiatives with one set of visuals, and speaking to our local and international audiences in the same language.

The SG:D logo is made up of rounded fonts that evolve from the expressive dot that is red. SG stands for Singapore and :D refers to our digital economy. The :D smiley face icon also signifies the optimism of Singaporeans moving into a digital economy. As we progress into the digital economy, it's all about the people - empathy and assurance will be at the heart of all that we do.

BROUGHT TO YOU BY

pdpc PERSONAL DATA PROTECTION COMMISSION SINGAPORE

IN PARTNERSHIP WITH

CSA SINGAPORE

AS PART OF

SG CYBER SAFE