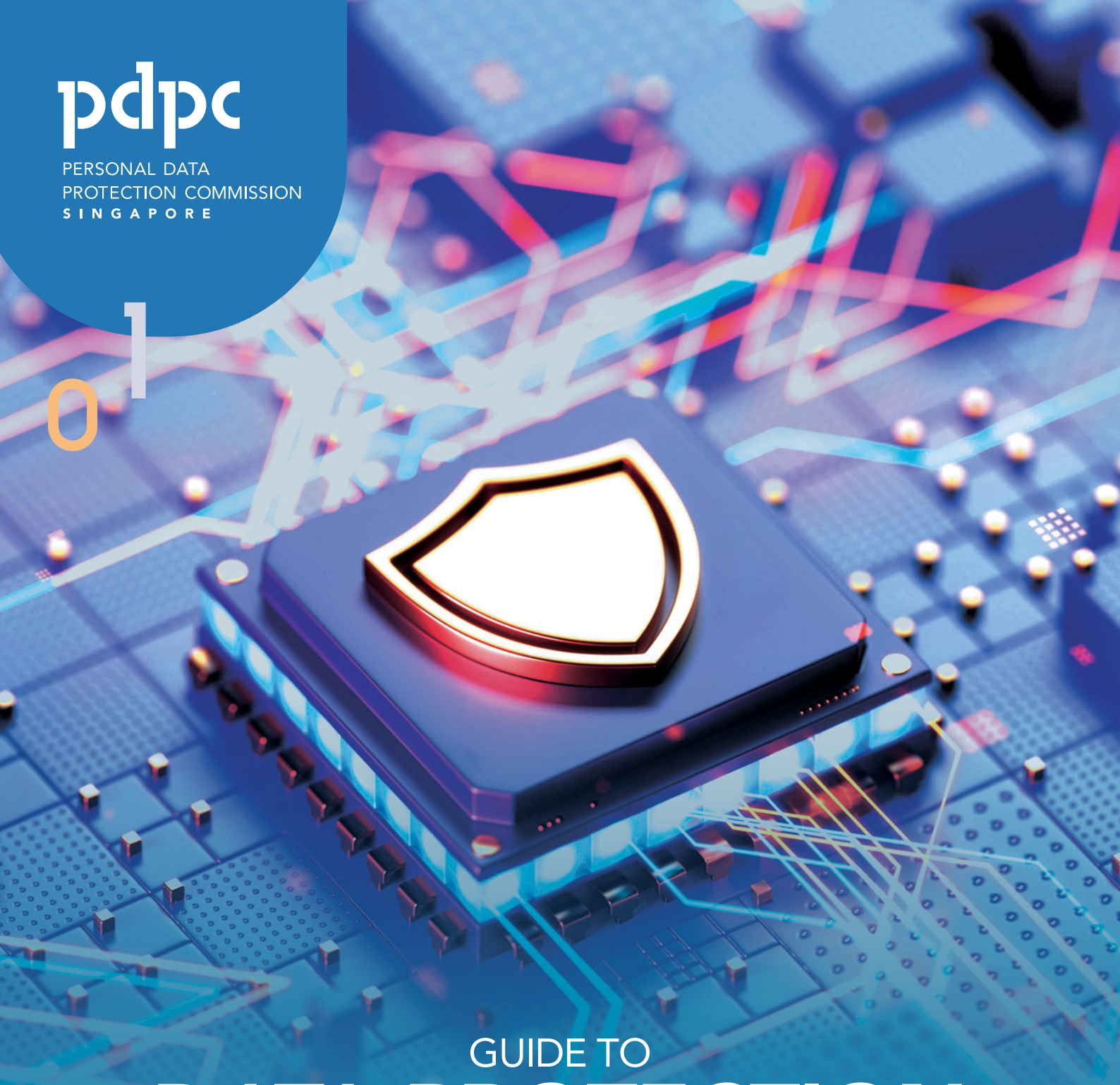
pdpc

PERSONAL DATA PROTECTION COMMISSION SINGAPORE



GUIDE TO

DATA PROTECTION PRACTICES FOR ICT SYSTEMS

Supported by

CSA SINGAPORE
Cyber Security Agency of Singapore

As part of

SG CYBER SAFE

Issued 14 September 2021
Revised 20 July 2026

CONTENTS

INTRODUCTION

INTRODUCTION

In the face of increasing risks of data breaches 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 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.

This guide also references the cyber hygiene practices in the Cybersecurity Agency of Singapore's ("CSA") Cybersecurity Certification: Cyber Essentials Mark ("Cyber Essentials"). The practices in the guide are organised into categories similar to those in Cyber Essentials, for ease of adopting the data protection best practices to cyber hygiene practices.

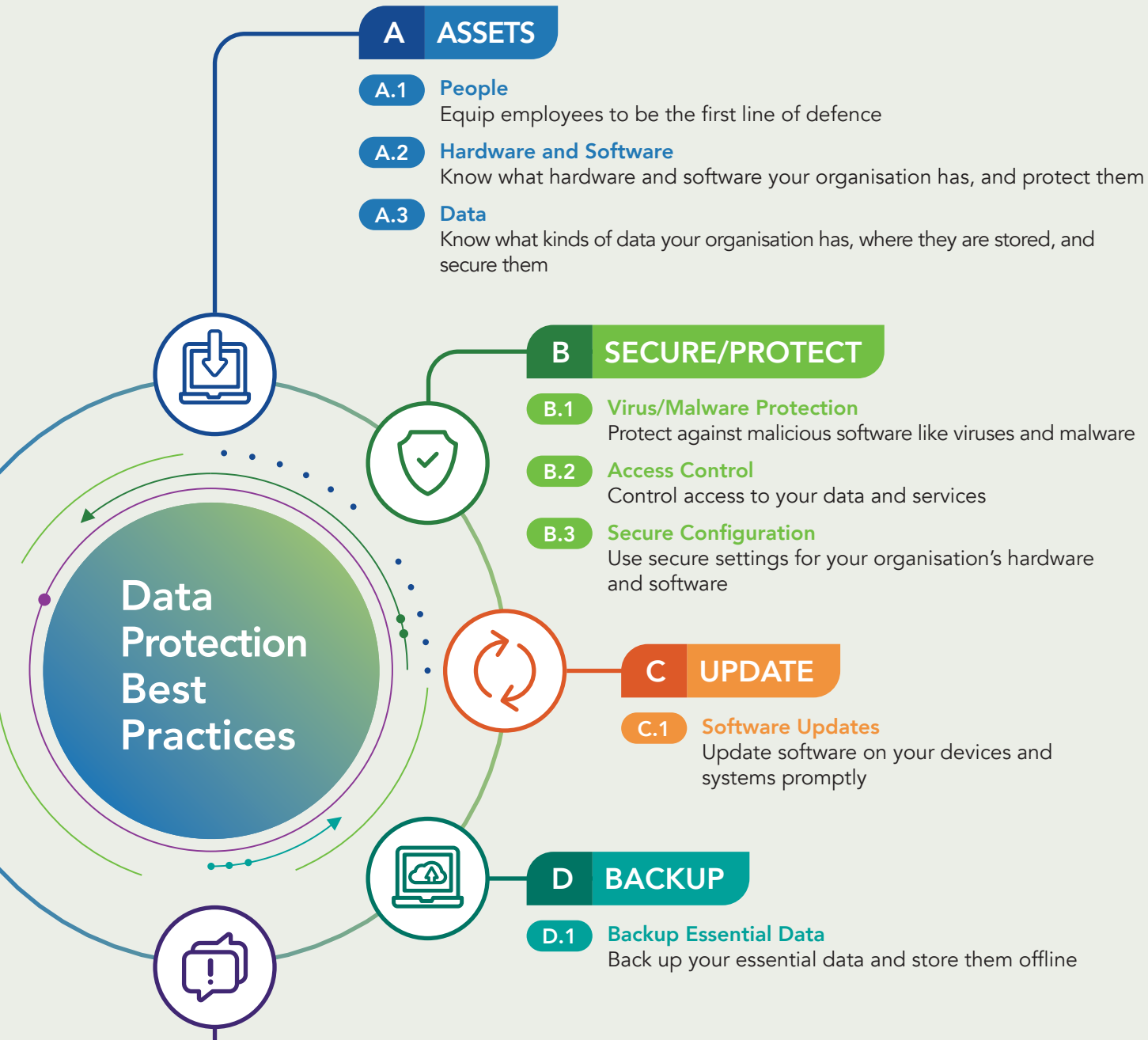
As Artificial Intelligence ("AI") rapidly transforms industries and delivers immense benefits, its growing adoption also introduces significant risks, including adversarial attacks, data breaches, undesired model outcomes, AI bias and hallucinations. While the field of AI security remains nascent, it is essential that organisations adopt robust best practices and governance frameworks to ensure AI systems behave safely and as intended. Given the rapid pace of AI development, system owners must remain vigilant, continuously apprising themselves of the latest data protection developments and refreshing their risk management strategies to harness the full potential of AI with confidence and trust[1]. To this end, this guide contains practices that organisations can consider and implement when adopting or using AI systems.

The best practices 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, i.e. basic practices. This guide is intended as a living document and will be updated to ensure its recommendations remain relevant.

[1] *Refer to PDPC's Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. (See Additional Resources)*

DATA PROTECTION BEST PRACTICES FOR ICT SYSTEMS

The data protection best practices for ICT systems are organised into the categories shown below.



A ASSETS

A.1 People
Equip employees to be the first line of defence

A.2 Hardware and Software
Know what hardware and software your organisation has, and protect them

A.3 Data
Know what kinds of data your organisation has, where they are stored, and secure them

B SECURE/PROTECT

B.1 Virus/Malware Protection
Protect against malicious software like viruses and malware

B.2 Access Control
Control access to your data and services

B.3 Secure Configuration
Use secure settings for your organisation's hardware and software

C UPDATE

C.1 Software Updates
Update software on your devices and systems promptly

D BACKUP

D.1 Backup Essential Data
Back up your essential data and store them offline

E RESPOND

E.1 Incident Response
Be ready to detect, respond to, and recover from cyber incidents

Each category recommends the basic and enhanced practices that organisations can put in place for their ICT systems. 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[2] to the individual, they should implement the additional relevant enhanced practices suggested in each section. The design and implementation of these protection measures should always consider the sensitivity of the data based on the nature of the business and services offered. Organisations should always bear in mind the principle of data minimisation and consider the necessity of retaining personal data in its original form.

[2] *These personal data could include:*
- *Personal data used for transactional or authentication purposes, e.g. credit card info;*
- *Personal data that may result in the adverse impact on individuals if disclosed, e.g. health-related data or financial-related data;*
- *Children's personal data.*

A ASSETS

A.1 People

To actively instil cybersecurity awareness among employees across all levels within the organisation, as they are your first line of defence. In addition, encourage the cultivation of a culture of shared responsibility in cybersecurity within the organisation.

Ensure proper governance over the employees of the organisation to create a data protection and cybersecurity culture with (a) clear accountability, (b) standards, policies and procedures that are effective, (c) security awareness, (d) risk management (including implementing processes to check for and remove accounts and credentials of ex-employees once they have left the organisation), and (e) processes to rectify and address non-compliance.

Organisations are to communicate and inform their staff about their data protection policies and inculcate an organisational culture of responsibility among staff through regular training and awareness programmes.

Increasing training and awareness of ICT security threats and protection measures among employees, as well as ensuring that appropriate internal policies and processes are updated and in place, helps to reduce the risk of data breaches through system misuse or mistakes. An example of such training and awareness includes being vigilant against malware, phishing, and other forms of social engineering. This can be fostered through mandatory cybersecurity briefings for new joiners and regular refreshers for all staff. Where employees have unrestricted Internet access, they should also be made aware of the organisation's security policies and standards governing its use.

Case Study 1: Importance of Cybersecurity Awareness

A technology consultant and solution provider fell victim to a cyberattack, with the threat actor compromising the company's email systems. The threat actor subsequently used the compromised company's email address to send phishing emails to the company's customers. Later investigations found a general lack of security awareness amongst the employees of the company, including the importance of authentication measures. This was partly the reason why a weak password was set in the email account, which allowed the threat actor to exploit this by performing brute force attacks on it. This incident resulted in unauthorised access to the personal data of individuals.

Security Awareness

The use of weak passwords suggests employees lacked a fundamental understanding of password security principles. This case demonstrates the need for security awareness training as it serves as the first line of defence by educating personnel about common attack vectors, social engineering tactics, need for security policies and basic security hygiene practices.

Good ICT Security Policies

Comprehensive ICT security policies establish clear standards for passwords and passphrases[3], access controls, system configurations and incident response procedures. These policies provide the foundation for consistent security practices across the organisation and ensure accountability at all levels. Having robust security policies can help in preventing cyberattacks.

Risk Management Framework

A comprehensive risk management framework enables organisations to systematically assess their threat landscape, identify vulnerabilities in their systems and processes, and implement appropriate controls based on risk appetite and business impact.

[3] *A passphrase is a memorised secret consisting of a sequence of words or text that used in authentication, rather than solely relying on random characters. A passphrase functions like a password in use but is generally longer for added security.*

Data Protection Best Practices

1 The Senior Management of an organisation is responsible for its data protection objectives and needs to provide clear directions on data protection policies for ICT systems within the organisation, which are to be documented.

2 Data protection risks can be managed through ICT controls. Close collaboration is necessary between data protection and ICT security functions within an organisation. This should be evident at appropriate levels of its governance structure (e.g. IT Steering Committee, Board of Directors, Change Management Committee).

3 An organisation is required to develop and implement ICT security policies for data protection in areas such as:

- Access control;
- Asset management;
- Information transfer;
- Secure configuration and handling of user devices;
- Information classification and handling;
- Network security;
- Information security incident management;
- Backup;
- Cryptography and key management;
- Management of technical vulnerabilities; and
- Secure development.

Organisations should develop and implement policies appropriate to their context, accounting for factors like the type and amount of personal data they collect, and the purposes of such collection. The policies will provide the employees who own or are responsible for managing the ICT systems with the direction and guidance they require for all ICT system implementations and activities related to data protection in ICT systems, in accordance with business objectives and the relevant laws and regulations.

4 Periodically review and update ICT security policies, data protection policies, standards and procedures to ensure continued relevance, adequacy and effectiveness. Each review can account for the latest regulatory and technological developments and audit findings so that data protection polices stay current and robust.

5 Communicate ICT security policies to both internal stakeholders (e.g. staff) and external parties (e.g. customers, third-party service providers). This assures external stakeholders that their personal data is 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.

6 Institute a risk management framework[4] 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. Such threats/risks should include cyber incidents arising from human factors such as AI-enabled social engineering and deepfake attacks, and the use of corporate and/or personal devices for work, i.e. bring your own device ("BYOD").

The risk management framework should include implementing processes to check for and remove accounts and credentials of ex-employees once they have left the organisation.

7 Periodically assess the effectiveness of the risk mitigation controls. Examples can include putting these mitigation controls through regularly structured internal audits[5] or performing security testing to check that the mitigating controls indeed function as expected.

8 Assess and mitigate the security risks involved in outsourcing or engaging external parties for ICT services. When engaging a data intermediary, organisations remain accountable for personal data processed on their behalf. This means that organisations should exercise due diligence and ensure that the data intermediary complies with the Personal Data Protection Act ("PDPA"), including the adoption of appropriate measures to manage their data intermediaries[6]. As an on-going effort, organisations should ensure that the external parties providing ICT services adopts a high standard of care and diligence in protecting personal data and system resilience.

Security Awareness and Training

9 Educate employees on the organisation's ICT security policies, data protection policies, control measures and procedures for the protection of personal data through regular awareness and training programmes (i.e. courses or online videos). Training and awareness programmes are essential to equip employees with the knowledge needed to effectively implement data protection policies and practices for ICT systems, fostering a culture that is sensitive and alert to data protection issues and concerns. Where feasible, the training and awareness content should be differentiated based on employee roles[7].

10 Conduct periodic (e.g. annual) ICT security awareness training to keep employees updated on common topics such as password and passphrase management, phishing/social engineering protection, corporate/personal device protection and reporting cyber incidents. Put in place processes to monitor the awareness level of the employees and the training effectiveness. The training programme should be reviewed periodically to ensure its content remains current and relevant.

[4] *Refer to PDPC's Data Protection Management Programme or CSA's Cyber Trust Mark on how to get started with risk assessments based on common risk scenarios. (See Additional Resources)*
[5] *Refer to CSA's Cyber Essentials Mark's self-assessment checklist to understand your current cyber readiness to jumpstart towards a more structured regular audit regime based on your implemented best practices and controls. (See Additional Resources)*
[6] *Refer to PDPC's Guide to Managing Data Intermediaries. (See Additional Resources)*
[7] *Refer to PDPC's E-Learning on Data Protection. (See Additional Resources)*

11 Conduct regular social engineering simulation exercises such as phishing, vishing, smishing and business email compromise simulations to remind employees to be alert to phishing emails[8] and other forms of social engineering.

When Adopting AI Systems

12 Perform a risk assessment, focusing on security risks related to AI systems. This should be done in a manner similar to existing risk management process of the organisation or based on best practices. Organisations should then address the risks identified and implement relevant measures to secure the AI systems.

13 Have in place clear written policies and document processes in relation to the safeguards for personal data that are collected and processed by the AI systems (e.g. end-user prompts, inputs and generated outputs, agent or tool activity data, internal enterprise data).

14 The organisation's employees or vendors that are involved in developing or implementing AI systems are to be trained with the knowledge needed to effectively implement data protection policies in development, such as through secure coding practices and the good practices for the AI lifecycle[9].

15 Educate users on the proper use of AI systems, including the security and data risks associated. For example, to highlight what specific types of data or documents that should be input into the systems and how data flows through the AI system.

Security Awareness

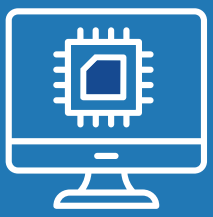
16 Keep updated on current data protection practices and incorporate best practices and industry recommendations into the organisation through means such as threat intelligence subscription services, data protection or cybersecurity newsletters, or participation in data protection community forums. This includes, but is not limited to, lessons from data breach findings[10], cybersecurity exploits such as from Common Vulnerabilities and Exposures ("CVE")[11], phishing and their mitigation strategies.

[8] *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.*

[9] *Refer to online resources from OWASP AI, and CISA: https://owaspai.org and https://www.cisa.gov/resources-tools/resources/secure-by-design*

[10] *For data breaches in Singapore, refer to PDPC's Enforcement Decisions. (See Additional Resources)*

[11] *Refer to the CVE site: https://www.cve.org*



A.2 Hardware and Software

To actively manage the hardware and software assets within the organisation's environment. Having asset visibility enables the implementation of effective monitoring and protection measures. Active asset management also ensures that only authorised assets and devices are used and that only authorised software is installed.

Visibility over the hardware and software assets used in processing and storing personal data will allow organisations to identify and know which assets to protect.

Organisation's hardware assets can include servers (e.g. email, web, Domain Name System ["DNS"], and application servers), networking and security devices and appliances (e.g. firewalls and routers), end-user devices (e.g. desktop computers, laptop computers, portable and mobile devices like tablets and mobile phones). Software assets include business applications, online services accessed using business email and other applications accessed locally or remotely via devices.

Case Study 2: Importance of ICT Asset Management

A Singapore-based organisation suffered a ransomware attack which resulted in having the personal data of individuals that it held to be encrypted. Investigations found that the threat actor gained access to the organisation by exploiting vulnerabilities from the Internet-facing servers that had reached End-of-Support ("EOS") status. The attack entry point allowed the threat actor to move laterally within the organisation's network to other servers that contained personal data within the organisation using compromised user credentials.

Good Asset Management Practices

This case demonstrates how having good asset management can help prevent data breaches. In this case, where there are End-of-Support systems, they pose significant security risks as they no longer receive security updates or patches from vendors, leaving known vulnerabilities permanently exposed. By allowing these systems to remain operational and Internet-accessible, it allows a larger attack surface that threat actors could readily identify and exploit.

Data Protection Best Practices

1 Conduct physical asset inventory checks regularly to ensure that all computers, software and other electronic devices (e.g. mobile devices, IoT devices, portable hard drives, printers, fax machines) used to store or process personal data are up-to-date and accounted for. This would include the proper disposal of assets (e.g. decommissioned server and software) and planning for asset replacement/upgrade (e.g., EOS software and hardware). Organisations can consider automating the checks by using software tools to identify, inventory and track these hardware and software ICT assets, which may identify the presence of a "shadow IT".

Document the asset inventory list using tools such as IT management software or spreadsheets and record the network diagram of the ICT assets to allow for proper tracking and maintenance.

2 Document all software functional and technical specifications (e.g. programme 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.

3 Maintain and periodically review (e.g. twice per year) the asset inventory list of all the hardware and software assets, including those from vendors. Ensure there is a process to regularly check for and update patches (see C.1 for details) for these assets.

For the asset inventory list, consider including the tracking of third-party software and tools; and expiry dates of all digital assets such as certificates, software licenses and software renewal to allow for timely renewal.

4 Unauthorised hardware and software assets, or those that have reached their respective EOS dates, should be removed.

When there is continued use of EOS assets, the organisation should assess and understand the cybersecurity risk, apply mitigating measures to address the risk, obtain approval from senior management, and monitor it until the asset is replaced.

5 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 fewer software programmes installed on a computer, the lower the likelihood that vulnerabilities are present.

6 Before redeploying, exchanging or disposing of any hardware asset, ensure all personal data is securely wiped, sanitised, or otherwise destroyed, e.g. perform cryptographic erasure by discarding or erasing the full-disk encryption key of a hard disk or Solid-State Drive ("SSD"), before reformatting and overwriting it.

7 When disposing of hardware assets, implement secure disposal methods, e.g. destroying the hard disks physically, incinerating, degaussing or engaging disk-shredding services.

When Adopting AI Systems

8 Maintain an inventory of AI systems in use across the organisation. For each system, the inventory should capture its purpose, data flow information and intended users, and be reviewed and updated regularly. As AI becomes increasingly integrated into business operations, these systems form part of an organisation's strategic assets, where having a clear inventory of these systems enables organisations to manage and secure them accordingly and helps mitigate against the risks associated with "shadow AI".

A.3 Data

To actively manage data in the organisation's environment, including identifying and maintaining an inventory of personal data in the organisation. Having a holistic visibility of the types of data the organisation collects, processes and stores enables the implementation of effective monitoring and protection measures to prevent unauthorised access and/or disclosure.

Collection of Personal Data

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

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.

Managing Consent

Consent can be obtained in a few different ways. In accordance with good practice, an organisation should obtain consent in writing, or have it 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.

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 is 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.

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—for example, during software migration or development. This includes 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 can result in a data breach.

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, minimise the volume of personal data kept, consider methods to anonymise personal data or use privacy enhancing technologies.

Personal Data in ICT Systems

ICT systems, including personal computers, portable devices such as notebooks, tablets and mobile phones, and removable storage media like USB drives and memory cards, are commonly used in organisations for work purposes and often contain personal data stored locally during normal operations. These devices and media, particularly portable and removable ones, face heightened risks of being misplaced or stolen compared to desktop computers. This makes them more susceptible to unauthorised disclosure, modification, removal or destruction of personal data. Therefore, organisations implement appropriate security measures, including encryption, to protect personal data stored on all computing devices and storage media, regardless of whether they are company-issued or employee-owned devices under BYOD policies.

Personal Data Stored With Cloud Service Providers

Cloud computing offers agility, efficiency and flexibility for companies of all sizes to consume technology wherever the businesses may be located and allows for 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. For example, the maintenance and control of infrastructure upgrades. Additionally, patching and system administration used to be performed by the organisation's IT team, but in cloud systems, such duties are no longer performed by its own IT team, but rather the cloud provider, which is a third party. 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 of the data being 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.

Case Study 3: Employing Appropriate Measures to Protect Data

A medical institution suffered a significant ransomware attack that resulted in the exfiltration of approximately 12GB of data. The breach originated from a critical buffer overflow vulnerability in the organisation's firewall, which had remained unpatched for two years. This flaw allowed a remote threat actor to bypass authentication and enter the network. Once inside, the attacker laterally moved within the network, as there was a lack of threat detection, and eventually gained access to thousands of individual personal data records, which contained individuals' information such as account details and credit card numbers that were stored in the clear. The threat actor eventually performed exfiltration of data into the dark web before deploying the ransomware, which encrypted the organisation's data.

Encryption of Personal Data

Encryption acts as the final line of defence. Even if a threat actor successfully exfiltrates files, robust encryption ensures that personal data remains unreadable and commercially useless. Organisations should prioritise "encryption at rest" for data containing personal data and "encryption in transit" for data moving across networks.

Data Minimisation and Housekeeping

Data minimisation helps to reduce a threat actor's "attack surface" on the available data that can be compromised. Organisations should practice conducting periodic checks for personal data stored in ICT systems and securely disposing of data that is no longer required or anonymise the personal data. This would have reduced the volume of personal data at risk.

Data Classification and Management

Not all data is created equal. A tiered classification system allows organisations to apply more stringent security controls over personal data compared to public-facing data. Had this been implemented, the organisation would have identified certain types of data, such as credit card information, as higher risk and requiring additional protection measures, potentially implementing further security safeguards such as network segmentation, enhanced monitoring, and stricter access controls.

Data Loss Prevention ("DLP")

This case highlights the importance of monitoring large data transfers, which often include personal data. Unexpected large data transfers are an important indicator of compromise that necessitates urgent cyber intervention. The key lesson is that organisations should implement proactive data loss prevention measures, including continuous monitoring of data export activities and establishing automated thresholds for allowable transfers. When suspicious activity or threshold breaches are detected, network controls should immediately block data packets at firewalls to prevent further exfiltration. Organisations should also consider dedicated DLP tools, which provide comprehensive data classification, monitoring, and automated prevention capabilities across all network endpoints. Had such measures been in place, the attackers' ability to transfer sensitive data to the dark web could have been prevented, significantly reducing the impact of this breach.

Data Retention Policies

The safest data is the data you no longer store. Only retaining data you need helps organisations limit the data to protect, and that can potentially be lost. Organisations must implement strict retention policies that mandate the permanent deletion or anonymisation of personal data once it is no longer required for legal or business purposes.

Data Protection Best Practices

Classify and Manage Personal Data

1 Identify, classify and manage data repositories or datasets containing personal data by considering the potential adverse impact (e.g. reputational or financial) on the individuals involved should the data be compromised by maintaining an inventory of personal data. Methods can include using spreadsheets or asset inventory software. The inventory list can contain details of the data, such as description, data classification, sensitivity, location and retention period.

The organisation should also document the data flow diagram for personal data in all ICT systems holding substantive personal data and develop and implement a data protection and security policy covering these areas.

2 Conduct a Data Protection Impact Assessment[12] ("DPIA") before development to assess the types of personal data and the data processing activities, and if AI systems are used or adopted for achieving the purposes of a new ICT system.

3 Conduct periodic checks (e.g. annually or when there are changes to the datasets) for personal data stored in ICT systems. For personal data that is no longer required, securely dispose of the data. If there is a need to retain the data beyond its retention (e.g. for performing longitudinal data analytics), archive them in an anonymised or in aggregated form. Consider employing privacy-enhancing technologies to meet these objectives.

[12] *Refer to PDPC's Guide to Data Protection Impact Assessments. (See Additional Resources)*

4 Implement measures to prevent employees, third parties and contractors from disclosing or leaking personal data outside the organisation. Examples include:

- Disabling USB ports;
- Including clauses regarding unauthorised disclosure of information in employment contracts and contractual agreements with third parties or contractors[13]; and
- Incorporating Extended Detection and Response ("XDR") end point solutions that are contextually aware of the content stored within files and documents which can detect sensitivity within them to prevent transmission over authorised channels, such as emails or saving to cloud storage.

Collection of Personal Data

5 Practice data minimisation by not collecting personal data unless it is to be used and there is a 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.

6 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).

7 Personal data can be inadvertently collected in the form of metadata (e.g. Exchangeable Image File Format ["EXIF"] data in image files). Consider not collecting such data or removing them if they are not needed and check that removal or redaction processes are irreversible.

8 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 be automatically and continuously obtained.

9 Avoid repeatedly collecting the same data at different stages of an interaction, such as during the account registration process.

Notification of Purpose

10 Maximise your touchpoints 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.

[13] *Refer to PDPC's Guide to Managing Data Intermediaries. (See Additional Resources)*

11 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.

12 When sending notifications to the targeted audience, choose the most appropriate channels or approaches (e.g. in writing, through a form, on a website, infographics, orally or in person) that best suits the context of the business.

Managing Consent

13 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. selected by default).

14 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.

Access, Correction and Accuracy of Personal Data

15 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. This can be done in pop-up windows in apps.

Housekeeping of Personal Data

16 Protect temporary files, such as interface files or data migration files, while they exist and remove them once they are not required.

17 Implement a routine schedule to identify and remove temporary files when they are no longer needed.

Retention of Personal Data

18 Have an appropriate personal data retention policy which sets out the varying minimum/maximum retention periods for personal data contained in data repositories (which can include, but is not limited to, databases, files and documents, and data backups and archives) of ICT systems. ICT controls could be implemented in ICT systems to enforce retention periods, especially for organisations that hold a large quantity of personal data.

19 Where there is a need to keep the data beyond the retention period, review and anonymise records[14] to prevent the re-identification of an individual.

20 Delete records that are no longer needed, including temporary files created during software migration or development. The organisation can implement ICT systems to flag records that have reached the end of the retention period.

Personal Data in ICT Systems

21 Encrypt personal data that is stored at rest whenever possible. This includes 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.

22 Encrypt personal data that is transmitted in-motion whenever possible. This includes using industry accepted protocols, e.g. Transport Layer Security ("TLS") and Secure Shell ("SSH") when transmitted over the network during backup or migration.

23 Monitor data export activities to detect data exfiltration and consider configuring a threshold for allowable data export. Where possible, prevent data (such as blocking or dropping data packets at firewalls) from leaving the organisation once data exfiltration is detected or allowable data thresholds have been reached.

24 Minimise storage of personal data on portable computing devices and removable storage media. Erase personal data that is no longer required as soon as possible.

25 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).

Personal Data Stored With Cloud Service Providers

26 Cloud service providers can 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.

27 Keep the encryption keys secure and separate from where the encrypted data is. There are several methods to consider when doing so. For example, storing encryption keys on premises while personal data is in the cloud or utilising commercial key management solutions from a third-party vendor.

[14] *Refer to PDPC's Guide to Basic Anonymisation. (See Additional Resources.)*

When Adopting AI Systems

28 Be aware of the datasets used by the AI systems throughout the AI lifecycle. Datasets range from those that are to be used for the training and fine-tuning of the AI system as well as datasets that are to be used to run inference (e.g. generate new outputs). For these datasets, assess whether sensitive data or personal data is really required and classify them accordingly similar to those of other ICT systems.

29 Be aware of data protection obligations with respect to the collection and use of datasets by the AI systems, and make the necessary arrangements and take measures,[15] such as notifying users on the intended use of their personal data and obtaining meaningful consent.

30 Cease to retain personal data once the purpose for collection is no longer served and retention is no longer necessary for legal or business purposes. Where there is a need to preserve training data for future model development, organisations need to develop and make available a data retention policy that includes the rationale for longer retention periods and to regularly review whether retained personal data is still needed.

31 Organisations should encrypt sensitive datasets that are to be used by the AI systems when data is at rest, in transit and in use (if possible) wherever practicable.

32 Monitor and validate input prompts, queries or API requests for attempts to access, modify or exfiltrate information deemed confidential by the organisation.

Collection of Personal Data

33 Keep copies of consent messages, as changes made to the text can result in different versions with different effective dates. Keeping copies allows for easy checking of the exact message used on a certain date and time. Such records can be useful in the event of disputes with users.

34 Maintain a consent register to keep a record of what users have and have not consented to, and when the consent was obtained. This can be achieved via a consent management system.

[15] *Refer to PDPC's Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. (See Additional Resources)*

Access, Correction and Accuracy of Personal Data

35 Provide users with a self-management facility to allow them to manage their own personal data. This minimises the possibility of human error and reduces employee effort and time.

Personal Data in ICT Systems

36 Periodically review the method of encryption (e.g. Advanced Encryption Standard ["AES"] algorithm with a minimum of 256-bits key length for long-term retention periods) used in the ICT system 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.

37 Consider installing security technologies (e.g. DLP), which prevents the unauthorised transfer of data from a computer or network.

38 Enable remote device locking and wiping features for portable computing devices that contain or are able to access large volumes of personal data.

B SECURE/PROTECT

B.1 Virus and Malware Protection

To ensure adequate protection measures are in place to continuously monitor and defend against malware as it can compromise network access and cause damage to the organisation's environment.

Malware that is designed to steal data can enter the organisation through end-user devices (e.g., desktop computers, laptops, as well as portable and mobile devices such as tablets and mobile phones), network devices (e.g. firewalls, routers), non-standard computing devices (e.g. IoT devices), and servers (e.g. email, web and application servers) including cloud-hosted systems. Detection and protection measures that are deployed at these entry points can protect organisations from malware that could compromise personal data. It is important that organisations ensure that the detection and protection measures are not only installed but actively maintained across all ICT assets with regular updates to malware definitions and security configurations. Doing so sustains effective protection throughout their lifespan.

Case Study 4: Need for Layered Network Defence

A cloud-based solutions provider suffered a significant data breach, which put at risk approximately 120,000 individuals' personal data. The incident involved the unauthorised access to and the deletion of their client's personal data from their cloud servers. Investigations revealed that the organisation's web application was highly vulnerable to Structured Query Language ("SQL") injection attacks that allowed the threat actor to exfiltrate personal data from its databases.

Implementing Web Application Firewalls ("WAF")

For organisations offering web applications or Software-as-a-Service (SaaS), standard network firewalls are often insufficient at protecting against sophisticated application-level attacks. A WAF is vital because it monitors and filters web traffic to block application-level attacks that network firewalls may not. Without a WAF, an organisation remains exposed and vulnerable to common SQL injection threats.

Implementing Layered Network Defence

Additionally, organisations should not downplay the need to implement a layered network defence to address other network-related threats. By integrating multiple independent security layers—such as deploying a WAF, creating network-level segmentation to limit lateral movement and the spread of ransomware, and allowing only trusted access through VPN's, an organisation creates multiple barriers that a threat actor must overcome. This layered approach slows down the attackers' movement within the network, providing the organisation with crucial time to detect and prevent data breaches.

Data Protection Best Practices

Malware Protection

1. Virus and malware protection solutions should be installed on endpoints (e.g. laptops, mobile devices, IoT devices) to detect anomalous malware behaviour in real-time and provide constant protection. The virus and malware solution should be configured to scan and block the execution of suspicious files, prevent unauthorised remote connections, and restrict access to sensitive files, personal data and folders. It can do so through the real-time monitoring of system processes, network traffic, and file activity for Indicators of Compromise ("IOC") typically associated with the malware.

2. 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 to detect newer malware. Software updates help to patch security flaws and protect the documents/personal data on the computer.

3. Employees should install and use only authorised software and access only attachments from official or trusted sources to ensure the integrity of the software, e.g. code signing.

4. Employees should immediately report any discovery of:

   - Suspicious emails or attachments; and
   - AI security concerns or unexpected AI behaviour.

   The aforementioned are to be reported to the IT team and/or senior management for further investigations and the process is to be formally documented as part of the data breach management plan that is further elaborated in E.1.

Protecting Computer Networks from Malware

5 Firewall configuration settings and tests can take reference from industry best practices (e.g. Center for Internet Security ["CIS"], Open Web Application Security Project ["OWASP"], National Institute of Standards and Technology ["NIST"]) and vendor (e.g. Microsoft, Amazon, Google) recommendations on secure configurations.

6 Ensure that the firewall ports are closed by default and open them when necessary for operational purposes. Conduct event-driven (e.g. major changes to the ICT environment such as decommissioning of servers) and periodic (e.g. annual) reviews of firewall rules to restrict connectivity to only authorised/whitelisted servers/IP addresses and close all unused ports.

7 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).

8 Maintain a list of whitelisted connections to only allow connections to specific, trusted hosts, and review for any unnecessary external connections to undertake measures. This includes disabling overseas connections or implementing geofencing to limit connections to those from the jurisdictions of operations if they do not meet business needs.

9 Design and implement the internal network segmentation with multi-tier or network zones, segregating the internal network according to function, physical location, access type, etc. This allows network traffic to be controlled and filtered between the network zones, limiting lateral movement and the spread of ransomware in the event that one part of the network zone is compromised.

10 ICT systems containing repositories of personal data should be restricted from direct access to the Internet and protected behind firewalls or properly segmented in a network zone for such purposes.

11 Employees should use trusted network connections for accessing the organisation's data or business email, e.g. mobile hotspot, personal Wi-Fi, corporate Wi-Fi and Virtual Private Network ("VPN").

Protecting Web Applications and Websites from Malware

12 Scan user uploaded files for malware and perform follow-up actions upon detection of malware. Restrict user uploads to certain whitelisted file types that the organisation can have in use, as whitelisted file types can vary from one organisation to another.

13 Use a WAF to defend against typical web application attacks such as SQL injection and Cross-site Scripting ("XSS") attacks on the organisation's web application or website. WAFs can act as another layer of security in addition to security hardenings made at the application code level. The choice of implementation, whether to be deployed on-premises or SaaS-based WAF, is left to the organisation and their evaluation of its feasibility, efficiency and protection needs.

14 WAFs with signature-based detection should have their signatures and rules updated regularly to mitigate current application attacks.

15 WAFs should be used for monitoring any attempts at data exfiltration by monitoring outbound traffic for any suspicious activity. This can consist of large payloads or communications with blacklisted IP addresses.

When Adopting AI Systems

16 Ensure AI systems' input and output are protected with appropriate network and web security measures similar to those of other ICT systems.

17 Perform regular malware scans of AI systems to ensure that its models and data do not have malware embedded.

18 Organisations should monitor and log inputs and outputs to AI systems to prevent misuse or the AI system being tricked into incorrect or unintended responses. This would also facilitate audit and investigation.

Protecting Malware from Computer Networks

19 Deploy technical detection and preventive controls (e.g. Intrusion Detection System ["IDS"], Intrusion Prevention System ["IPS"] solution and XDR) to mitigate malicious activities. Organisations should consider updating and enhancing these technical controls using threat intelligence tools or feeds through automated rule updates, managed security service providers or cloud-based platforms that support functionalities that translate threat data into actionable security configurations.

20 Monitor the network, e.g. Local Area Network ("LAN")/Wi-Fi, regularly and remove unauthorised clients and rogue Wi-Fi access points.

21 Use network proxies or web security gateways to restrict employee access to known malicious websites.

B.2 Access Control

To ensure adequate protection measures are in place to limit access to the organisation's environment by employees and other third parties, including contractors and ex-employees.

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, and to remove such rules when no longer required, for instance, when an employee leaves the organisation. For administrative accounts, it is necessary to have stronger requirements, which include strong passwords/passphrases and 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 can be easily guessed by hackers. Hence, accounts and passwords need to be managed securely.

Case Study 5: Need for Strengthening of Access

An e-commerce organisation and its subsidiary suffered from a massive data breach that affected 200,000 of its former and existing customers. Investigations found that a threat actor gained access to the organisation and its subsidiary through the Internet-facing web management consoles. The threat actor got in by means of exploiting login credentials that accepts weak passwords belonging to one of the authorised accounts. This gave the threat actor access into the sales report function that aided in the exfiltration of personal data.

Implementing Secure Access

This case highlights the need for organisations to properly secure and manage access, including the enforcement of robust password and passphrase policies across the ICT systems. Passwords and passphrases must not include easily obtainable personal information such as names, NRIC numbers or birthdates. Additionally, in the event of a suspected data breach or cybersecurity incident, account passwords must be changed immediately to prevent further unauthorised access.

Deploying Multi-Factor Authentication (MFA)

A major preventative measure in this case is implementing MFA for administrative access to ICT systems and database servers. Even if threat actors had successfully compromised a user's password or passphrase through phishing, credential stuffing or brute-force attacks, MFA would have prevented unauthorised access to the management consoles. The attacker would have been unable to provide the second authentication factor, effectively stopping the breach at the initial access stage.

Data Protection Best Practices

1. Ensure access is granted to all accounts based on the principle of least privilege to prevent the granting of excessive privileges, e.g. where employees access only the information and systems required for their job.

2. Implement access control at the application level to restrict access to data to an authorised role.

3. Have clear policies that prohibit the sharing of passwords and passphrases, such as admin credentials, publicly displaying passwords or passphrases on Post-it notes or storing passwords or passphrases in public web folders (including GitHub). Conduct periodic audits (e.g. clean desk inspection) to detect such undesirable practices.

4. Use of administrative accounts should be monitored through logs generated or alerts received to ensure they're used properly and not for non-administrative activities.

5. Ensure that outsourced vendors are aware that their services will involve handling personal data, and that they understand their responsibilities and requirements for data processing. Under the PDPA, organisations remain accountable for personal data processed by data intermediaries on their behalf and are responsible for ensuring these intermediaries uphold the same data protection standards[16]. This requires exercising due diligence to ensure data intermediaries comply with the PDPA, including adopting appropriate cybersecurity arrangements.

   Access granted to outsourced vendors should be limited to the information and systems necessary for their role and revoked when no longer required. Outsourced vendors must also notify the organisation of any data breaches involving personal data processed on the organisation's behalf.

[16] *Refer to PDPC's Guide to Managing Data Intermediaries. (See Additional Resources.)*

6 ICT system administrators can use system notification services to be notified in the case of suspicious activities, such as the creation of user accounts outside of office hours or by non-administrator accounts.

7 Maintain an inventory of accounts and regularly review (e.g. quarterly or when there are changes to the account list) to ensure all active accounts are valid and being assigned with proper rights. Remove or disable invalid or inactive accounts (e.g. inactive for more than 60 days). Organisations should implement processes to remove accounts and credentials of ex-employees promptly.

8 For both users and administrators of ICT systems, change all default passwords and replace them with a strong passphrase (it should be at least twelve [12] characters long, including upper case, lower case and/or special characters). A passphrase consists of words or text used in authentication and functions like a password in use, but is longer for added security. Passwords and passphrases must not include personal information such as names, NRIC numbers or birthdates, or other information that can be obtained easily. In the event of any suspected data breaches or cybersecurity incidents, account passwords are to be changed.

Where feasible, the organisation should implement additional measures to assist employees with secure password or passphrase management, e.g. passphrase or password managers, passwordless authentication.

9 For both users and administrators of ICT systems, passwords, passphrases and/or secrets that are used for authentication to systems or services by either human or machine are not to be stored in the clear (or in plaintext), or in public repositories, e.g. GitHub. An example of human-used authentication includes passwords and passphrases stored as plaintext file notes on the user's workstation computer, while an example of machine authentication are API keys that are not to be stored in the clear publicly.

10 Administrators of ICT systems will need MFA when accessing ICT systems and database servers containing personal data. MFA requires administrators of ICT systems to authenticate using a combination of two or more of the following methods:

- something you know (like a password or passphrase)
- something you have (like an authenticator application that delivers a One-Time-Password ["OTP"] or a smart card)
- something you are (like your fingerprint or face)

11 User and administrator accounts are to be disabled and/or locked out after multiple failed login attempts, e.g. ten failed login attempts or rate-limiting attempts[17].

[17] *This means that the time the user needs to wait between attempts increases with each failed login attempt.*

12 When performing remote administration to servers such as through Remote Desktop Services/Protocol ("RDS"/"RDP"), virtual desktop infrastructure, Virtual Network Computing ("VNC"), telnet, or terminal services, consider applying additional controls. This can include restricting access to specified external IP addresses, geofencing and ensuring remote administration is performed behind a secured VPN or over encrypted channels.

13 Limit login attempts to mitigate automated brute force attacks, which include credential stuffing. ICT systems are to automatically block, or slow down users or machines attempting to login after a certain number of failed logins in a short period of time. Measures can include progressive delays between failed attempts, blocking the IP address of the offender or sending alerts to system owners or administrators to investigate further.

14 After system/software migration or a major change is made, check that access controls configurations and settings are correctly applied as intended.

For Personal Computers

15 Use an authentication mechanism before logging into an operating system, such as a passphrase. After a period of user inactivity, the screen should be locked, and authentication should be required to resume.

16 Prevent unauthorised personnel from viewing the screens of personal computers easily by using privacy filters, or through the positioning of personal computers.

Cloud Service Provider Considerations

17 Ensure that the CSP can adhere to a minimum standard by being International Organization for Standardization ("ISO") certified as necessary.[18] Relevant standards can include the latest published versions of ISO/IEC 27001,[19] ISO/IEC 27017,[20] ISO/IEC 27018,[21] MTCS SS 584[22], or other recognised international standards. Obtain a copy of the certification for your records if possible.

The organisation should review CSP practices for the following to ensure alignment with its requirements:

- Service Level Agreements ("SLAs") for cloud service availability, and the protection of data confidentiality and integrity; and
- Vulnerability assessment and penetration tests conducted by the CSPs.

[18] *Refer to Guide to Cybersecurity for Law Practices by The Law Society of Singapore. (See Additional Resources.)*
[19] *Refer to ISO Standards available at https://www.iso.org/standard/27001*
[20] *Refer to ISO Standards available at https://www.iso.org/standard/43757.html*
[21] *Refer to ISO Standards available at https://www.iso.org/standard/27018*
[22] *Refer to MTCS SS 584 Standards available at https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/IT-Standards-and-Frameworks/Cloud-Computing-and-Services*

18 Negotiate for the CSP's responsibilities by providing them with clear operational requirements (e.g. conduct third-party audits/penetration tests and share reports/ test results) and including these within the contractual agreements.

When Adopting AI Systems

19 Ensure that appropriate user access to the AI systems' (e.g. rule- or role-based access controls) development or deployment environment is based on the principle of least privilege, to limit who or what can view and process personal data.

20 Where the AI system (including those with agentic capabilities) has access to data, it is to be configured in accordance with its intended data or other systems' access according to the same principles of least-privilege. This applies to time-bound access as well; for example, if an AI system with agentic capabilities is expected to fetch data daily between 2am and 3am, its access rights should be restricted to that window only. This is to prevent any accidental access to or disclosure by the AI system to your personal data or systems containing personal data. The responsibility for protecting personal data remains with the organisation deploying the AI system.

Enhanced Practices

21 Implement segregation of duties to prevent an individual from executing potential conflicting responsibilities on their own (e.g. initiating, approving, and executing a change or requesting, approving, and implementing access rights). It is also desirable to have a job rotation and cross-training for security admin roles and functions.

22 When administering across multiple applications or services that require authenticated logins, consider using a Privileged Identity and Access Management ("PIAM") solution to manage credentials. This is done to minimise the risk of credential theft and misuse as it allows for the consistent enforcement of security policies over the lifecycle of credential management. PIAM that supports leaked credential monitoring should enable automatic remediation to immediately block detected leaked accounts or reset the authentication method before the account is compromised. PIAM can also provide a more convenient and improved login experience for administrators by allowing Single Sign-On ("SSO") logins on multiple applications or services.

23 Review the authentication token's validity period to ascertain if shorter durations can be set, based on how long users or administrators are expected to stay meaningfully logged on in the system.

For Personal Computers

24 Disallow anonymous or guest logins where the computer is deemed to contain sensitive personal data records.

25 Disallow non-administrator users from booting up a computer using external or removable storage media.

26 Disallow non-administrator employees from installing software or changing security settings, except under specific circumstances.

B.3 Secure Configuration

To ensure adequate protection measures are in place to secure the configurations and settings of hardware and software, thereby mitigating risks associated with exploits or vulnerabilities.

Database Security

Databases are used to store and manage data. Some of them 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 on the individual should such data be compromised.

Securing Websites, Web and Mobile Applications

Websites, web and mobile applications are often used to communicate or provide services to customers or the public regarding 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, web and mobile applications, which include malicious file uploads, 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.

ICT Security Assurance Testing

Organisations should always ensure that the protection of personal data and the security of the ICT system are part of the design considerations at each stage of the system development lifecycle. Otherwise, subsequent changes to the system to resolve any security breaches will incur more cost to the organisation. Organisations should always check that security rules remain valid after hardware and software migration or development.

Coding issues have been raised as the main cause of a number of data breach incidents that have occurred in 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.

Case Study 6: Need for Robust Application Security

An e-commerce organisation suffered from a severe data breach that inadvertently allowed the threat actor to scrape the personal data of 2.6 million users. The organisation prior to the incident, was undergoing a system migration and launched a public-facing Application Programming Interface ("API") to facilitate the process. Investigations found that during this deployment, a filter intended to restrict the API to only publicly available information was unintentionally omitted. This "API Bug" created a critical vulnerability that allowed the API to call up personal data of its customers, which the threat actor misused.

Securing Websites and Applications

System migrations are high-risk activities where configuration settings can be inadvertently lost or omitted. By maintaining comprehensive documentation of all API configurations and securing them with industry best practices such as the OWASP's Top 10 list of web application security risks applications, organisations ensure that migration teams have clear procedures. During migration, documented configurations serve as checklists to verify that all security controls are properly transferred to the new environment. This practice would have ensured that the API filter requirement was clearly documented and verified during the migration process.

If external vendors are involved in system migrations or API development, organisations must ensure these vendors follow secure development practices. Regular audits of vendor security processes can identify gaps in documentation, testing or configuration management before they result in vulnerabilities. This practice establishes accountability throughout the supply chain.

Database Security

Even if application-layer vulnerabilities exist, proper database architecture provides defence-in-depth protection. By positioning databases behind firewalls and within isolated network segments, organisations can limit unauthorised access to sensitive data. This approach ensures that direct queries to database tables must pass through additional security controls rather than allowing unrestricted access to the underlying data stores.

Database-level access controls can restrict which data fields are accessible to specific API service accounts. Even if an API filter is omitted at the application layer, database column-level security can prevent non-public fields (such as email addresses, phone numbers or dates of birth) from being returned in query results. This creates a secondary defence layer that operates independently of application code.

ICT Related Testing

To ensure security measures are properly implemented, organisations should establish comprehensive security testing to detect misconfigurations and system vulnerabilities. This includes code reviews and thorough unit testing to identify missing data filters before deployment, while penetration testing specifically targeting APIs verifies that proper access controls and data filtering are enforced. Employing automated deployment processes with built-in validation checks eliminates human error by ensuring critical security configurations are consistently applied across all deployments.

Data Protection Best Practices

1 Enforce security configurations for all ICT system assets, including desktop computers, servers, routers, and when there are AI tools and services deployed. Methods can include adopting industry recommendations and standards, running baseline security analysers and securing the system configuration, e.g. using scripts.

NOTE — One of the organisations that offer security configuration guidelines is the CIS.

2 Document configuration settings, security policies and review/test these regularly during/post-system migration to ensure that they correspond and are applied to the current requirements. This includes allowed services, APIs, protocols, ports and compensating controls.

3 Implement email filtering on your organisation's corporate email to better detect and filter phishing or other types of malicious emails.

Securing Database

4 Securely configure databases and 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. Organisations can take reference from industry best practices (e.g. CIS, OWASP, NIST) and vendor (e.g. Oracle) recommendations on secure configurations.

5 Check that the database is secured and not placed in a vulnerable spot within the network and that it is not publicly accessible. For example, the database should be placed behind a firewall or in a different network segment away from the Internet.

6 Where practicable and when the functionality exists, encrypt database repositories or datasets containing 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.

Securing Websites, Web and Mobile Applications

7 Web applications can be securely configured by taking reference from vendor or industry recommendations such as the OWASP[23] "Top 10" list, which aims to addresses the most common security risks to web applications.

[23] *Website at https://owasp.org*

8 Unused features, services, or applications should be disabled or removed, e.g. disable file sharing services, File Transfer Protocol ("FTP") services and restrict software macros. Do not enable auto-run features of non-essential programmes (other than backup or virus and malware protection solutions).

9 Enable automatic lock/session log outs after fifteen minutes of inactivity for ICT systems.

10 Ensure that the system validates all data input by users so that no unexpected inputs can be keyed in through the user interface.

11 Ensure proper website session management and cookie controls[24]. Cookie attributes to secure include enabling "Secure", "HttpOnly", "SameSite", "Expire" and "Max-Age". Additionally, pay attention to session ID or token life cycle, session expiration and caching.

12 Ensure that files containing personal data are not accidentally made available on a website or through a web or mobile application. For example, avoid storing personal data in public folders or disabling directory browsing to prevent hackers from finding those files. Do not store secret API keys in public directories. Enable periodic scans for the presence of public folders on the website or web application and conduct periodic reviews of public folder contents. Apply automatic purging of contents within a public folder after a pre-defined retention period.

13 Do not allow "backdoors" in the form of "secret" URLs or debugging logs that allow access to personal data without user authentication.

14 When the web application is publicly accessible over the Internet, ensure its sensitive folders, especially those that contain personal data, remain hidden and are enforced with strict access control policies that are constantly monitored for unauthorised access. These measures should be used in conjunction with the web application's documentation on restricting indexing, web scraping, search engines, or AI bots, such as "robot.txt". However, do not solely rely on these documented restrictions to hide webpages or folders, as these restrictions may not be respected by the search engines or AI bots.

15 Apply the latest secure connection technologies or protocols that are supported by the ICT system or implementation. For instance, use Transport Layer Security ("TLS"), rather than Secure Sockets Layer ("SSL") for websites, web and mobile applications when handling personal data.

16 Perform website, web and mobile application scanning and source code analysis to help detect web vulnerabilities. Vulnerabilities to look out for could include those in the OWASP "Top 10" list or similar.

[24] *More information can be found on OWASP Session Management Cheat Sheet.*

17 Do not allow the use of multiple sessions by 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.

18 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 the online documentation provided and change the necessary configurations from the default setting such that data collected in forms are not published in a publicly accessible table.

19 When engaging vendors, ensure that vendors protect their own software, applications and environments used in the delivery of the engaged service.

Consider reviewing the cybersecurity posture of vendors or perform audits when necessary, so as to adequately manage supply chain risk.

NOTE — In Singapore, Cyber Essentials and Cyber Trust are certifications that help organisations to implement cybersecurity.

ICT Related Testing

20 Do not use or store production data that contains personal data in non-production[25] environments for testing or other purposes. Do not use production data for System Acceptance Tests ("SAT"). Organisations can consider creating test data from production data using anonymisation techniques.

21 Perform thorough impact analysis of any software or code changes and design before coding. This provides an accurate understanding of the proposed changes and its implications, which helps in making informed business decisions. This includes areas of the system that can be affected due to the change in the application's features.

22 Conduct code review and rigorous unit testing, which includes complete testing of functional requirements to verify compliance with the requirement specifications at an early stage in the system development lifecycle.

23 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 can result in leakage of sensitive personal data.

24 Conduct regression testing and system integration testing, which includes complete testing of both functional and non-functional requirements, and verifying the integration of the interfaces to all its external systems in the middle stage of the system development lifecycle.

[25] *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.*

25 Conduct SAT, 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 SAT, are properly planned to simulate real-world usage and be as comprehensive as possible. The SAT coverage should also include foreseeable exception handling scenarios, especially when personal data is being transmitted or displayed in these 'live' scenarios.

26 Perform security testing[26] (such as vulnerability assessment, penetration testing or red teaming) on the ICT system and production environment before commissioning to detect and resolve any vulnerabilities before going 'live', promptly after going live, periodically and upon major changes.

27 Prioritise remediation identified vulnerabilities that have a risk rating of "High" and above. The risk rating should be based on industry best practices as well as consideration of potential impact. For example, the criteria for the rating can include consideration of the Common Vulnerability Scoring System ("CVSS")[27] base score, and/or the classification by the vendor, and/or impact to application functionality.

28 Ensure that secrets (such as passwords, passphrases, keys or tokens) 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.

29 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, and in deploying the new build to the wrong environment, such as deploying a test build to the production environment.

30 Encrypt exported data and communicate the password or passphrase separately to the target recipient of the exported data (i.e. internal or external party).

Understanding Cloud Service Providers' Security

31 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. Implement the secure configuration best practices and/or settings published by its CSPs, if available.

[26] *Where organisations engage external service providers for security testing, they are to use licensed service providers. https://www.csro.gov.sg/resources/licensed-service-providers/*

[27] *The CVSS is a technical standard for assessing the severity of vulnerabilities in ICT systems.*

32 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.

33 Understand and leverage relevant CSP's native security services or offerings that can be used to better protect your organisation's existing CSP-hosted services or storage. For instance, services for identity management, authorisation, authentication and protected stores.

Security Logging

34 Log successful and failed logins with timestamps in order to assist detection or investigation into hacking attempts.

Should there be a legitimate purpose to include any forms of personal data in logs, the organisation is to employ adequate protection measures, such as data minimisation techniques, e.g. masking identifiable data to only show the minimally required information or encryption to protect these logs.

35 Log all database activities, such as any changes to the database and data access activities, to track unauthorised activities or anomalies.

36 Enable ICT system's security logging and monitor for timely detection of suspicious or malicious activity, e.g. unusual administrative activities during off peak hours, creation of unknown administrator accounts, escalating privileges for user accounts, lateral traversal across multiple segments and attempted download/upload by single system within a short period, disabling security controls such as disabling the audit log, web application attacks like an SQL injection, etc.

37 For all logs that generate alerts related to security, organisations should put in place a plan for responding to and investigating these alerts in a timely manner.

When Adopting AI Systems

38 Consider hardening AI systems[28] when appropriate, as it helps mitigate and be resilient against AI attacks, such as input-based attacks and prompt inject attacks at its core.

[28] *Refer to MITRE ATLAS techniques on Model Hardening: https://atlas.mitre.org/mitigations/AML.M0003*

39 Consider the evaluation of dependent software libraries and open-source models and, when possible, perform source code analysis. This ensures the implemented libraries does not have arbitrary code execution when being imported or used. This can be done by using a vulnerability scanning tool or checking against a database with vulnerability information.

40 Consider implementing appropriate privacy-enhancing technologies to protect and enable trusted data use[29] in AI systems after weighing the trade-offs of privacy-utility.

41 Before deploying or after any updates prior to releasing AI systems for production use, consider testing[30] and benchmarking them so they function as expected, Additionally, ensure that the integrity and authenticity of the released AI systems can be validated by users.

42 Where AI systems have agentic capabilities, organisations should:

- design and implement technical measures in the agentic AI system to mitigate identified risks to how agents function and operate;[31]
- thoroughly test agents for safety and security before deployment, covering areas specific to agents such as task execution, policy adherence and tool use accuracy across varied datasets to ensure expected behaviour;[32] and
- roll out agents gradually and monitor them in real time prior to deployment as their autonomous nature and changing environments make it difficult to anticipate all outcomes in advance.[33]

Securing Database

43 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.

Security Logging

44 Log access to sensitive personal data. Consider using a centralised log server (for example, Syslog) to collect such logs.

[29] *Refer to IMDA's Privacy Enhancing Technologies Adoption Guide. (See Additional Resources)*
[30] *Refer to IMDA's Starter Kit for Testing LLM-Based Applications for Safety and Reliability. (See Additional Resources)*
[31] *Refer to IMDA's Model AI Governance Framework for Agentic AI on considerations for suitable measures in section 2.3.1. (See Additional Resources)*
[32] *Refer to IMDA's Model AI Governance Framework for Agentic AI on considerations for suitable testing measures in section 2.3.2. (See Additional Resources)*
[33] *Refer to IMDA's Model AI Governance Framework for Agentic AI on considerations for suitable controlled roll-out and continuous monitoring measures in section 2.3.3. (See Additional Resources)*

45 Logs should be stored out-of-band from the ICT system or at secure locations to protect its integrity and ensure the availability of the logs.

46 Put in place a regular log review process to detect suspicious activities and early indicators of security violations, as well as possible breaches. Consider implementing security monitoring mechanisms that monitor all security related events for the timely detection of suspicious events or malicious activities.

ICT Related Testing

47 Have processes or systems in place to scan, detect, identify and address the ICT system's vulnerabilities. Proper vulnerability management of ICT systems deployed in both the production and testing environments will allow organisations to stay secure against exploits of these known vulnerabilities.

48 When performing vulnerability assessments for ICT systems, consider scanning not only public-facing servers but also interconnected internal servers within the organisation's network. Doing so helps with the discovery and mitigation of exploitable vulnerabilities that could impede an attacker's lateral movement within the internal network.

49 Before deploying the ICT system into production, consider testing it in a staging/pre-deployment environment that closely mimics production, to ensure it functions as expected.

When Adopting AI Systems

50 Consider staging AI systems under development in environments separate from production systems. This segregation may help isolate system misconfigurations, vulnerabilities or data corruption introduced during development from propagating to production environments.

C UPDATE

C.1 Software Updates

To ensure the timely application of updates and patches to software and applications, thereby safeguarding devices and systems against security vulnerabilities.

Having a regular software patch regime will ensure that software vulnerabilities are regularly patched as software vendors release security fixes. Doing so will prevent cyberattacks against known software vulnerabilities, which can lead to personal data being compromised. Maintaining regular assurance checks help organisations ensure that ICT security controls developed and configured for the protection of personal data are properly implemented and practiced.

Case Study 7: Need for Comprehensive Patching

A professional services firm suffered a ransomware attack that encrypted the personal data of approximately 550,000 users. Investigations found that the threat actor gained initial access to the network by exploiting a VPN account belonging to a user who was no longer employed by the firm. The threat actor then exploited system vulnerabilities across multiple unpatched systems within the firm to laterally move within the network, allowing the identification of where the personal data resides, before deploying the ransomware.

Importance of Patch Management

This case demonstrates the necessity of patch management, where the impact of a ransomware attack would have organisations comprehensively patch their entire ICT system and not be selective in patching, as gaps in patching will allow weaknesses or vulnerabilities in unpatched systems to be exploited. When immediate patching is not operationally feasible, assess the risk and apply appropriate compensating measures would help in limiting the threat actor to the initial entry point.

Data Protection Best Practices

Basic Practices

1 Prioritise the implementation of critical updates for operating systems and applications (e.g. security patches), obtained from official or trusted sources (e.g. verified through hash or checksum), as soon as is feasible.

2 Monitor for ICT system vulnerabilities through trusted vulnerability disclosure sites[34] or through vendors that provide ICT system vulnerability disclosure services.

3 Conduct compatibility tests on operating systems and application updates before installation.

When Adopting AI Systems

4 When AI systems are updated, test and validate that the output remains authentic and that any guardrails in place (e.g. input and output filters) remain effective to mitigate the risk that changes to the AI model may lead to unintended changes in behaviour.

5 Where AI systems have agentic capabilities, organisations should, throughout the AI systems lifecycle, implement change management and version control processes. In complex agent ecosystems, changes to one agent can have cascading effects across interconnected workflows. As such, organisations should define clear triggers that initiate a change review process and categorise the needed changes accordingly.[35]

Enhanced Practices

6 Enable automatic updates for security-related patches to receive the latest security-related fixes where feasible, and the deployment can be staggered into stages, starting with a subset of the organisation's assets.

7 Select vendors and their solutions that have a track record of or practice to notify its customers of the availability of updates/patches and delivering those updates/patches to their customers in a secure and prompt manner. If possible, guide/assist its customers to ensure the updates/patches are implemented successfully.

8 When immediate patching is not possible or feasible, consider implementing vendor-provided mitigations, or alternative mitigations applicable to the vulnerability, such as adapting or adding security controls (e.g. firewalls or at network borders).

[34] *Trusted vulnerability disclosure sites include https://cve.org*
[35] *Refer to IMDA's Model AI Governance Framework for Agentic AI on considerations for robust change management in section 2.3.3. (See Additional Resources)*

D BACKUP

D.1 Backup Essential Data

To ensure the regular backup of all essential business information in a secure manner to enable the organisation to restore and recover business operations following cybersecurity incidents.

Ransomware attacks can lock organisations out of their data, as the ransom can cripple the organisation's ability to function. These attacks are more common in data breaches where data backups play a critical role in protecting both personal and the organisation's data.

Case Study 8: Need to Protect Data Backups

A cloud hosting and enterprise software provider experienced a ransomware attack after a threat actor exploited its vulnerability in an End-of-Support firewall to gain initial access via a compromised administrative account. Once inside the network, the attacker specifically targeted the organisation's recovery capabilities by breaching the backup server, creating unauthorised administrative credentials and deleting stored backup data to prevent a swift restoration of services. The threat actor then encrypted the organisation's server environment, causing a total loss of system availability for its corporate clients and impacting internal corporate data.

The Vital Role of Robust Backup Policies

This case underscores a critical lesson, where backups are only as valuable as their protection from threat actors. When attackers successfully deleted the organisation's backup data, it exposed fundamental weaknesses in their backup strategy. A robust backup strategy should include these elements: backup frequency, protection mechanisms, backup retention and business recovery objectives.

Equally important is the isolation of backup environments from production networks. Air-gapped or immutable backups serve as appropriate safeguards by ensuring that even when threat actors gain administrative network access, the organisation's data remains recoverable.

Data Protection Best Practices

Basic Practices

1 Ensure that personal data in the organisation's possession is regularly backed up according to its backup policy. Backups should be regularly tested and scanned for malware to ensure that the backup data can be effectively recovered and restored in time[36]. Backup frequency, as defined in the backup policy, can be aligned to your organisation's business requirements and data loss tolerance.

Backups should include ICT system configuration, source code and other important data. The backup process should be automated where feasible.

2 Backups should be protected from unauthorised access and restricted to authorised personnel only. Backups should also be stored separately, offsite, or isolated from the operating environment (e.g. password-protected USB flash drives, encrypted external hard disks, encrypted backups or tape storage at an alternative office location).

3 Frequent backups, e.g. daily or weekly, should be stored online to facilitate quick recovery, e.g. cloud backup storage.

4 The backup should be encrypted with cryptographic algorithms and key lengths that follow the latest recommendations from industry standards, e.g. NIST or equivalent.

Enhanced Practices

5 Establish backup strategies aligned with the business Recovery Point Objective ("RPO") and Recovery Time Objective ("RTO"), e.g. determine and implement the scope and frequency of data backups that can sufficiently meet and recover from a disaster.

In business continuity processes, RTO is the time duration within which the ICT systems is expected to recover from failure and resume service, while RPO represents the point in time, prior to a system disruption, during which an organisation must recover its data from the most recent backup copy. In defining the RPO, organisations must account for their obligation to protect personal data, ensuring that the maximum acceptable amount of data loss does not compromise their accountability to the individuals whose personal data they hold.

6 Implement a version control system where developers can roll back to a previous version in the event of any show-stopping bug being discovered.

[36] *Should the restored data contain personal data, organisations are to purge all personal data from the testing environment after completion of the test.*

E RESPOND

E.1 Incident Response

To ensure the organisation has an incident response plan that enables timely, professional, and appropriate detection, response, and recovery from cybersecurity incidents.

Development of a data breach management plan will enable an organisation to manage and respond to data breaches more effectively. The data breach management plan should also include processes for investigating and responding to alerts about suspicious incidents.

Case Study 9: Gaps in Incident Response Management

An HR services organisation experienced a ransomware incident that resulted in the exfiltration of approximately 5,500 individuals' salary information. Investigations revealed that the threat actor gained access to the organisation through a compromised account that provided remote access to its cloud environment. This threat actor remained active within the organisation and went undetected for two weeks due to the organisation's lack of an effective incident response capability.

Importance of a Data Breach Management Plan

Having a comprehensive data breach management plan in place would have significantly mitigated this incident's impact by establishing early detection procedures to identify compromised endpoints and suspicious access patterns before substantial data exfiltration occurred. This would define clear roles and responsibilities that ensure immediate escalation when security anomalies are detected, implementing structured communication and escalation pathways to apprise the correct stakeholders, and conducting post-incident reviews to systematically address vulnerabilities through policy updates and technical controls.

Basic Practices

Data Protection Best Practices

1 Develop a data breach management plan to manage and respond to data breaches more effectively. Such a plan should consider the organisation's business processes and needs and cover the spectrum of the use of data throughout its lifecycle[37].

The data breach management plan can include the following details:

- Clear roles and responsibilities for key personnel involved in the incident response plan process;
- Procedures for detecting, responding to and recovering from common cybersecurity threat scenarios, e.g. ransomware, social engineering, data breach, data exfiltration, accidental disclosure of data from the cloud, and employees' disclosure of sensitive organisational information to external AI tools or services;
- A communication plan and timeline for escalating and reporting the incident to internal and external stakeholders, e.g., regulators, customers or senior management; and
- Proper assessment of the data breach and reporting it to the PDPC if required[38].

The data breach management plan should be reviewed at least annually. Organisations can consider running tabletop exercise simulations of common threat scenarios to better prepare themselves to respond to data breaches in a prompt and effective manner.

2 The data breach management plan should be communicated to all employees with access to the organisation's IT assets, data and/or environment.

3 Post-data breach incident reviews should be conducted, and learning points should be incorporated back into the data breach management plan, data protection polices and ICT security policies.

Understanding a Cloud Service Provider's Escalation Process

4 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.

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

[38] *Refer to more details on the data breach notification process and timelines, which can be found in PDPC's Guide on Managing and Notifying Data Breaches Under the PDPA and PDPC's Advisory Guidelines on Key Concepts in the PDPA, Chapter 20. (See Additional Resources)*

ANNEX

ANNEX

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

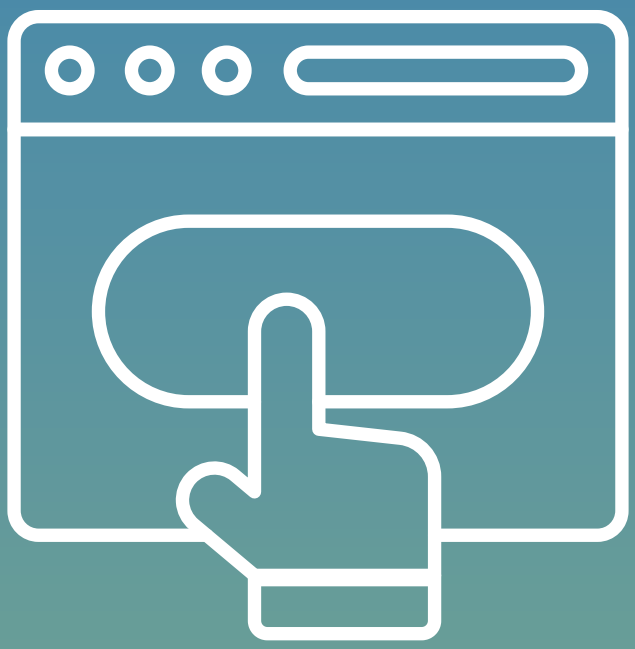
Checklist for Incident Response Management[39]

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, the current baseline of IT systems' activities, security logs, backups of important data, etc., to adequately scope out the response. This includes knowing where the inventory of ICT assets, such as hardware, software, and data repository are.					
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. Ensure action plans developed for responding to common incidents are accessible and all updates are communicated to the relevant parties. Ensure that all plans include considerations on proper security alert handling so that all security alerts are followed up on.					

[39] *This checklist is referenced from CSA's Incident Response Checklist. Please access the full checklist from CSA's website: https://www.csa.gov.sg/resources/singcert/incident-response-checklist*

Good ICT Practices	Practice Met				Action Plan
Basic Practices	Comply	Partial Comply	Not Comply	Not Applicable	
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. If backups or off-site logs are available, they can be used as a further resource for analysis.					
h. Be able to make an initial assessment and prioritise the next steps when affected by a cyber incident.					
i. Ensure the organisation has a Standard Operating Procedure ("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.					

Good ICT Practices	Practice Met				Action Plan
Basic Practices	Comply	Partial Comply	Not Comply	Not Applicable	
Containment, Eradication & Recovery					
k. Be 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 and passphrase length and complexity, tightening network perimeter security, etc.					
n. Recognise the need to continue monitoring their network for signs of intrusion and to maintain vigilance, even after the threat has been eliminated.					
Post-Incident Review					
o. Conduct 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, after the incident is resolved by the organisation.					



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.

PDPC Guides and Advisory Guidelines

- Advisory Guidelines can be found on the *PDPC website*.
  - Advisory Guidelines on Key Concepts in the Personal Data Protection Act
    - Chapter 17 (The Protection Obligation)
    - Chapter 18 (The Retention Limitation Obligation)
    - Chapter 20 (The Data Breach Notification Obligation)
  - Advisory Guidelines on the Personal Data Protection Act for Selected Topics
    - Chapter 7 (Online Activities)
    - Chapter 9 (Cloud Services)
  - Advisory Guidelines on the PDPA for Children's Personal Data in the Digital Environment
    - Chapter 6 (Protection of Children's Personal Data)
  - Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems
    - Part III (Using Personal Data in AI System Development, Testing and Monitoring)
    - Part IV (Deployment – Collection and Use of Personal Data in AI Systems)
  - Advisory Guidelines on Use of Personal Data in Generative AI
    - Part II (Development – Collecting and Using Personal Data to Develop Generative AI Models)
    - Part III (Deployment – Data Protection Responsibilities of Generative AI Stakeholders)
- *Model Artificial Intelligence Governance Framework*
- *Model Artificial Intelligence Governance Framework for Generative AI*
- *Model Artificial Intelligence Governance Framework for Agentic AI*
- *Guide to Developing a Data Protection Management Programme*
- *Guide to Data Protection Impact Assessments*

- *Guide to Managing Data Intermediaries*
- *Guide on Managing and Notifying Data Breaches under the PDPA*
- *Guide to Accountability*
- *Guide to Basic Anonymisation*

Education

- *E-Learning on Data Protection*

Other Information, Guides and Certifications

- *PDPC's Enforcement Decisions*
- *IMDA's Data Protection Essentials Framework*
- *Data Protection Trustmark SS 714:2025*
- *IMDA's Privacy Enhancing Technologies Adoption Guide*
- *IMDA's Starter Kit for Testing LLM-Based Applications for Safety and Reliability*
- *CSA's Certification for the Cyber Essentials mark*
- *CSA's Certification for the Cyber Trust mark*
- *CSA's Internet Hygiene Portal*
- *Guide to Cybersecurity for Law Practices*

BROUGHT TO YOU BY

PERSONAL DATA PROTECTION COMMISSION SINGAPORE

SUPPORTED BY

CSA SINGAPORE
Cyber Security Agency of Singapore

AS PART OF

SG CYBER SAFE