

ANNEX A: EXISTING GOVERNMENT EFFORTS IN USING DATA SECURELY

1 The Committee focused on data security, rather than cybersecurity, as there are ongoing work streams to strengthen the Government's cybersecurity posture. The Committee's work built on existing efforts by the Government to improve its data security and cybersecurity standards.

2 The Committee recognises that the Government has been actively strengthening data security and cybersecurity in the public sector, even prior to the formation of the Committee. Some examples of these data security and cybersecurity initiatives include:

- a. The introduction of Internet Surfing Separation policy in 2016;
- b. Disabling of USB ports from being accessed by unauthorised devices in 2017;
- c. Increase in the types of IT audits around data management in 2017; and
- d. Measures to detect and respond more quickly to cyber threats that target critical Government databases in 2018

Box A1: Difference between Data Security and Cybersecurity

Data security refers to the process of protecting the confidentiality, integrity and availability of **data**. This is different from cybersecurity, which is intended to maintain the confidentiality, integrity and availability of **systems**. While they are two distinct concepts, both data security and cybersecurity are closely linked and have overlapping elements.



An example of a cyber-incident is the Norsk Hydro cyber-attack, where intruders brought down Norsk's IT systems and website for 31 hours. Norsk was unable to connect to its production systems, affecting its operations significantly, even though no data was exfiltrated. On the other hand, an example of a data incident that is not a cyber-incident is when a public officer inadvertently sends a confidential email to unauthorised parties. Data was compromised even though no intruder infiltrated the IT system. There are incidents that affect both cyber and data security. An example is the SingHealth incident, where a cyber-attack resulted in the leak of the medical records of 1.5 million patients.

Government Data Security Policies and Legislation

3 Since 2001, the Government's data security policies have been set out in the Government Instruction Manual Policy on Data Management (IM8 PDM). The IM8 PDM also prescribes specific measures to protect Government data. All agencies are required to comply with the IM8 PDM. Public agencies are regularly audited for their compliance with the IM8 PDM requirements.

4 In April 2018, new data security provisions were included in the Public Sector (Governance) Act (PSGA) to further strengthen public sector data governance while facilitating cross-agency data sharing to improve policy-making and service delivery. The PSGA sets out the circumstances under which data should be shared across public agencies. The PSGA also imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or re-identify anonymised data.

Box A2: Differentiated data security regimes for the public and private sectors

The Personal Data Protection Act (PDPA) was enacted in 2012 as a baseline standard for data protection in the private sector, to boost trust in data management and processing, and thereby improve the economic competitiveness of Singapore. Public agencies are not governed by the PDPA, but under the PSGA and the IM8 PDM.

The need for two different legislations governing data management in the public and private sectors arises because the public has different expectations of the services provided by the Government and the private sector. The public expects the Government to deliver services in an integrated manner across agencies, but they do not expect this of the private sector.

For example citizens would expect the Ministry of Education to obtain personal data of children at the compulsory school age from the Immigration and Checkpoints Authority to ensure that they are enrolled in a primary school. A citizen would not expect a tuition centre to know what other tuition centres his child is enrolled in.

5 In November 2018, the Government introduced a new Information Sensitivity Framework (ISF) to ensure that data is appropriately protected. The Government collects and uses a broad range of personal and business data to serve citizens. Within this range of data, sensitive data must be treated with the appropriate level of care. For example, vehicle license data may be non-sensitive, while an individual's history of infectious disease may be highly sensitive and must be well-safeguarded. The ISF guides agencies to develop measures specific to the protection of personal and business data, and calibrates the data protection measures based on the severity of harm to individuals and entities upon unauthorised disclosure of the data. The ISF enables public agencies to have a consistent treatment of sensitive data which is necessary for inter-agency data sharing and data analytics.

Government Data Architecture for secure data sharing and usage

6 In October 2019, the Government introduced the Government Data Architecture (GDA) to enable secure data sharing and usage across the public sector. The GDA lays out the organisational structures and technical infrastructure required to facilitate efficient data sharing of clean and authoritative datasets across public agencies. It does so by designating and building:

- a. Single Sources of Truth (SSOTs) that acquire, clean and maintain high quality core data¹;
- b. Trusted Centres (TCs) that fuse and distribute core datasets; and
- c. Central platforms for data users to request, download and analyse datasets.

7 The TCs distribute only non-identifiable data for policy analysis and planning purposes, while identifiable data is used only for service delivery and operational purposes. The GDA enables the practice of good security habits by public agencies. It minimises the need for agencies to collect datasets on their own as they can obtain the same data from the Trusted Centres. Public agencies can also purge their datasets when they have finished using them, without fear that the dataset would no longer be available. This reduces duplicative work for public agencies and minimises the different attack points from which a malicious attacker can attempt to extract data.

8 The GDA promotes secure data sharing and usage by incorporating and industrialising data security safeguards across the Government. The GDA will incorporate the measures recommended by the Committee; its safeguards will be continually updated to ensure that data is well protected. Public agencies that use the GDA's central platforms enjoy a high standard of data security by default.

¹ Core data are data that are frequently used by multiple public agencies.

ANNEX B: INSPECTION OF AGENCIES' DATA MANAGEMENT PRACTICES – OVERVIEW OF APPROACH AND FINDINGS

1 The Committee carried out an inspection of 336 systems across 94 public agencies² to identify data security risk areas and common causes of data incidents. The objectives of the inspection were to: (a) assess agencies' compliance with data management policies and standards set out in the IM8, and (b) benchmark existing safeguards to industry and global best practices to further identify how policies and standards can be improved.

The Inspection Approach

2 The inspection of systems was conducted in two phases. Phase 1 of the inspection was conducted from April to June 2019 and focused on 5 agencies with highly-sensitive data and large volumes of data, namely, the Central Provident Fund Board (CPF Board), the Inland Revenue Authority of Singapore (IRAS), the Health Promotion Board (HPB), the Health Sciences Authority (HSA) and the Ministry of Health (MOH). Phase 2 of the inspection was conducted from June to October 2019 and covered the remaining 89 agencies.

3 In total, 336 out of 2,840 systems in Government were inspected. On average, 3-4 systems per agency were selected for inspection, based on a combination of the following criteria:

- a. **Security Classification** – systems classified as Critical Information Infrastructure (CII)³ systems were more likely to be selected.
- b. **Information Sensitivity** – systems containing highly-sensitive data and large volumes of data were more likely to be selected.
- c. **Risk Profile** – systems where sensitive data was stored in non-Government facilities, used in non-production environments and/or accessed by third parties, were more likely to be selected.

4 Results from Phase 1 of the inspections informed the Committee's recommendations to address gaps in the Government's data security regime. Findings from Phase 2 of the inspection were similar to those in Phase 1, and confirmed the relevance of the Committee's recommendations.

² The inspection covered all public agencies, with the exception of the Pioneer Generation Office, which was renamed as Silver Generation Office and joined the non-Government Entity Agency of Integrated Care (AIC) in April 2018. AIC is an independent corporate entity under MOH Holdings.

³ CII refers to a computer or computer system that is necessary for the continuous delivery of an essential service, and its loss or compromise will have a debilitating effect on the availability of the essential service in Singapore.

Findings of the Inspection

Non-compliance with Existing Policies and Standards

5 The Committee found that there was scope to improve agencies' data security practices. About 75% of agencies had at least one finding on non-compliance with IM8 policies and standards. 64% of agencies were rated "low-risk", 23% were rated "medium-risk" and the remaining 13% were rated "high-risk".⁴

- 6 The most common findings were in the following areas:
- a. Management and monitoring of privileged user accounts, particularly the review of privileged user activity logs;
 - b. User access reviews;
 - c. Encryption of emails with highly-sensitive data; and
 - d. Management of extraction of production data to non-production environments.

Adopting Industry and Global Best Practices

7 The Committee also looked at whether agencies adopted industry and global best practices that were not set out in the IM8. This was to identify areas where the Government's policies and standards could be improved.

8 The Committee identified the following best practices that the Government should incorporate in its data security policies and standards, for promulgation across the public sector:

- a. Training of officers and third party vendors to raise awareness and capabilities in managing data security risks and implementing data protection measures.
- b. Strong management of third party vendors to ensure that they protect Government data well.

Additional Observations from the Inspection

8 The Committee observed that there should be more emphasis on data security and data management during regular system audits. The learning points from the inspections should be used to improve the scope and process of the regular IM8 audits.

9 The Committee also observed that smaller agencies could be better supported to implement all the policies as intended. Smaller agencies tend to have smaller IT teams and fewer resources to implement data security measures. The provision of central IT services and central solutions can help them improve data security in a more cost-effective manner.

⁴ Agencies will rectify the inspection findings and GovTech will validate that these findings were rectified.

The Inspection Findings Informed the Committee's Recommendations

10 The findings from the inspections informed the Committee's recommendations, as follows:

No.	Findings	Recommendations that address these findings
Findings on Non-Compliance with Prevailing Policies/Standards		
1	Privileged User Management & Monitoring	<ul style="list-style-type: none"> • T4. Enhanced logging and active monitoring of data access • Implement central log review services.
2	User Access Review	<ul style="list-style-type: none"> • T2. Automatic Identity and Access Management (IAM) tools • P6. Limit and monitor authorized and privileged access
3	Email Encryption	<ul style="list-style-type: none"> • T12. Password protecting and encrypting files • P9. Securely distribute password out-of-band • T5. Email data protection tool • P10. Distribute files through appropriate secure channels. Agencies can share sensitive data files through Singapore Government Document Collaboration Service (SG-DCS).
4	Management of Production Data Extraction	<ul style="list-style-type: none"> • T4. Enhanced logging and active monitoring of data access
Global and Industry Best Practices to be Adopted		
5	Data Security Awareness Training	<ul style="list-style-type: none"> • Recommendation 3.2: Equip these key groups with the requisite competencies and capabilities to perform their roles effectively.
6	Third Party Management	<ul style="list-style-type: none"> • Recommendation 1.6: Enhance the third party management framework to ensure that third parties handle Government data with the appropriate protection.
Additional Observations		
7	Audit on Data Security Risks	<ul style="list-style-type: none"> • Recommendation 1.5: Enhance the data security audit framework to detect gaps in practices and policies before they manifest into incidents. Under this enhanced framework, systems with sensitive data will be subjected to more frequent audits.
8	Smaller agencies need more help	<ul style="list-style-type: none"> • Implementation approach: Recommendation that the Government build central platforms and provide central services where appropriate. This would also ensure greater consistency in implementation across agencies.

Note: Measures prefixed with 'T' are technical safeguards and measures prefixed with 'P' are process safeguards under Recommendations 1.1 to 1.3

ANNEX C: KEY RECOMMENDATION 1 - TECHNICAL AND PROCESS MEASURES TO PROTECT DATA AND PREVENT DATA COMPROMISES

Enhance technology and processes to effectively protect data against security threats and prevent data compromises

1 The Committee recommends 13 technical measures and 10 process measures to protect against data security threats, prevent data compromises, and maintain the confidentiality of data. The proposed technical measures must go hand in hand with complementary process safeguards to be effective. For example, password protecting a file can prevent access by unauthorised personnel, but will only be effective if the password is transmitted securely through a separate channel from the file.

2 Each technical measure and process measure is described with the following elements:

- a. Purpose of the measure;
- b. An example to illustrate how the measure works; and
- c. (for technical measures only) How the measure could be implemented.

Recommendation 1.1: Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads.

3 Surface area of attack describes the different points through which an attacker can try to extract data. Keeping the surface area of attack as small as possible reduces the likelihood that an attacker is able to compromise data.

4 **Collect and retain data only where necessary.** The Government should minimise its collection and retention of data to what is reasonably necessary or has value for agencies' operations:

Measure:	P1. Collect datasets only where necessary
Purpose:	Reduces the surface area of attack by minimising the collection of datasets that are unnecessary or have no clear identified value for agencies' operations.
Illustrative Example:	Agencies should not collect data that is already collected by Single Sources of Truth as part of the Government Data Architecture. Agencies should obtain such data from the Trusted Centres when needed.

Measure:	P2. Limit retention period of data
Purpose:	Reduces the surface area of attack by minimising the storing of datasets at agency or at endpoint devices.

Illustrative Example:	Agencies should set a retention period for each dataset collected. The datasets should be purged from the officer's laptop (and any backup copies) after the retention period is over.
-----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5 Minimise the proliferation of data to endpoint devices. Beyond minimising the collection and retention of datasets, the Government should also discourage excessive downloads of sensitive data. This reduces the risk of data being lost should an endpoint device be compromised.

Measure:	P3. Isolated secure environments for third parties and privileged users
Purpose:	Ensures that high-risk users (i.e. users which are entrusted with functions, tasks or data that are highly sensitive) are not able to extract data from Government systems.
Illustrative Example:	Suppose a vendor or public officer requires access to sensitive data to perform operations on behalf of the agency. Instead of downloading the dataset onto the vendor's system, the vendor or public officer accesses it through a Virtual Desktop Infrastructure (VDI) which prevents data transfer. The vendor or public officer is able to view the data required, but will not be able to copy out the data.

Measure:	P4. Access data by queries instead of data dumps
Purpose:	Reduces the risk that a full database is compromised as only the necessary fields are accessed.
Illustrative Example:	Suppose an officer requires a particular citizen's data for delivering targeted services. Instead of downloading the whole database with records for all citizens, the officer queries the database and retrieves only the record of the citizen that the officer is serving.

Measure:	P5. Access sensitive files on secured platforms
Purpose:	Ensures that access to sensitive files have the appropriate security safeguards and are logged and monitored.
Illustrative Example:	Suppose an officer needs to access a sensitive database. Instead of downloading data from the database onto his laptop, he should use the collaboration functions of the Singapore Government Document Collaboration Service (SG-DCS) to access data on the platform where feasible. This is the equivalent of accessing data on Google Drive without downloading it onto one's laptop.

6 Access and use data for the task at hand. Access should be limited to relevant datasets, or to a subset of the data so that the data users only have access to the data that is needed to carry out their assignment. This reduces the risk of an accidental exfiltration, or outside attacker gaining access to sensitive data through compromising a data user's account. This also reduces the risk of an insider accessing sensitive data when he or she is not authorised to do so.

Measure:	T1. Volume limited and time limited data access
Purpose:	Prevents officers from accessing too much data at one time, and the duration the officer can access it.
Illustrative Example:	Suppose a malicious actor gets hold of a public officer's laptop as well as the login and password. The malicious actor would not be able to access volumes of the data larger than the officer's predefined limit, and will not be able to access the dataset longer than the pre-set period of time (e.g. 24 hours) without reauthorisation. This mitigates the damage that the malicious actor could potentially cause.
Technical Implementation:	Restrict data access when the duration and volume data access exceeds predefined limits. This can be done using the access controls features of the ICT systems and in conjunction with logging and monitoring of data access.

Measure:	T2. Automatic Identity and Access Management (IAM) tools
Purpose:	Ensures that access to the data is limited only to people authorised to do so.
Illustrative Example:	Suppose an officer previously took on a role in a department that authorised him to access a database. When that officer relinquishes that role by moving to another department, the IAM will ensure that he will no longer have any access to that database.
Technical Implementation:	<p>IAM tools automatically manage officers' identity and access rights, ensuring that only authorised persons can access data.</p> <p>Automatic Privileged Identity and Management (PIM) tools control, monitor, and protect user accounts which have more access and capabilities than ordinary users (e.g. administrator accounts). More stringent measures (e.g. 2FA, time-limited access) are required to protect these accounts.</p>

Measure:	P6. Limit and monitor authorised and privileged access
Purpose:	Reduces the risk that a malicious outsider gains access to an account with access to sensitive data.

Illustrative Example:	Agencies should set strict processes that allow privileged access only where necessary, and ensure access is closely tracked and not shared. This includes immediate revocation of access and surrender of security tokens once a privileged user is terminated from employment or has changed job roles. This is enabled by the technical safeguard, T2: Automatic Identity and Access Management Tools.
-----------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Recommendation 1.2: Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity

7 Logging and monitoring allows the Government to detect suspicious or high-risk activity, and take immediate action to resolve this to prevent data compromises. This builds on other safeguards (e.g. P5: Access Sensitive Files on Secured Platforms) which ensures that data transactions occur on secured platforms where all access is logged and monitored.

8 Enhance logs and records to more accurately pinpoint high-risk activity and assist in response and remediation.

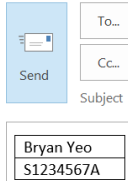
Measure:	P7. Maintain data lineage
Purpose:	Identify any unauthorised modification and usage of data flows, and support the remediation of an unauthorised modification to the data.
Illustrative Example:	Suppose an attacker maliciously changes a person's record in a database. By maintaining a record of where the data is used, how the data is transferred, how the data has been changed and who has used the data for what purposes, the agency is able to identify and rectify this unauthorised modification.

Measure:	T3. Digital watermarking of file
Purpose:	Enable investigators to trace from whom the dataset originated from in the event of a data incident.
Illustrative Example:	Suppose an officer downloads a dataset from a central repository. The dataset will have a watermark that is unique to the officer. In the event of a data incident (e.g. the dataset being posted on online forums), investigators will be able to tell from the watermark, which officer the dataset originated from. This will allow investigators to conduct better forensic analysis to identify how the incident occurred and prevent future data incidents.
Technical Implementation:	Adding marking information, such as cryptographic signature. The watermark information can identify the

	originator of the dataset, prove the authenticity of the file, and is hard to remove from the file.
--	-----------------------------------------------------------------------------------------------------

9 Detect suspicious activity and alert the user or stop the unauthorised activity automatically.

Measure:	T4. Enhanced logging and active monitoring of data access
Purpose:	Keep logs and analyse them to flag out anomalous activity as well as support remediation in the event of a data breach.
Illustrative Example:	Suppose a malicious actor performs an attack over a long period of time. The individual actions by the malicious actor at each point of time might not raise any red flags; however, his actions over time might be suspicious. By storing and analysing logs, these anomalous activities over time will be flagged out.
Technical Implementation:	<p>Logging of data access to sensitive data at greater detail, such as at the individual data query level. The logs should be protected from accidental or deliberate erasure, so that they can reliably show what data has been compromised, how it has been compromised and who was involved.</p> <p>Active monitoring of data access to sensitive data by proactive scanning of log files for anomalous data access behaviours, and active checking of data access endpoints' for compliance with data security rules.</p>

Measure:	T5. Email data protection tool
Purpose:	Ensures email senders double-check that they intend to send any email with potentially risky activities (e.g. containing sensitive data, or to suspect addressees) to prevent any accidental or unauthorised disclosure through email.
Illustrative Example:	<p>Suppose an officer is sending an email with sensitive data (e.g. NRIC).</p>  <p>When he/she clicks "Send", a pop-up will appear asking for confirmation that he/she intends to send such information to the recipient parties. The email will be sent out only upon the officer's confirmation.</p>

Technical Implementation:	Email tools which scan for potentially risky activities (e.g. embedded files in file attachments, large numbers of users in cc lists, email content contains identifiers such as NRICs) and require users to positively affirm that they intend to proceed with the potentially risky activities.
---------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

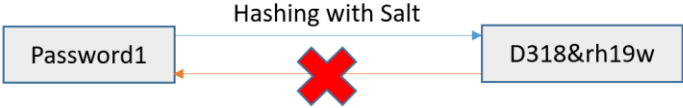
Measure:	T6. Data loss protection tools
Purpose:	Prevents anomalous activities that are likely to be correlated with malicious activity or data incidents.
Illustrative Example:	Suppose a malicious external actor gets hold of a public officer's laptop and credentials. Using the officer's laptop, the malicious actor tries to download large amounts of sensitive data. This raises red flags and the file transfer is automatically stopped.
Technical Implementation:	Monitor computer network and files for anomalous activities (e.g. unexpected downloads of large amounts of data to personal computers) and stop any unauthorised file transfers.

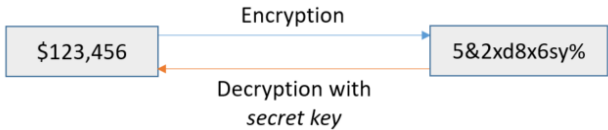
Recommendation 1.3: Protect the data directly when it is stored and distributed to render the data unusable even if extracted.

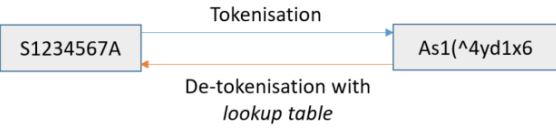
10 Cybersecurity defences provide a strong layer of defence to prevent malicious users from accessing the data within IT systems. In the event that IT systems are compromised, the intruder will have access to the underlying data and can use them for his/her malicious purposes. The Committee thus recommends applying an additional layer of protection on the data itself (e.g. encrypting the data) to render the data unusable to the hacker even if the IT system was compromised. This approach significantly reduces the likelihood of a single point of failure leading to data compromise. In technical parlance, this is referred to as “defence-in-depth”.

11 **Render data unusable even if exfiltrated from storage.** This ensures that even if an attacker were to break into the IT system, the data would be unusable to the attacker.

Measure:	T7. Hashing with salt
Purpose:	Ensure that sensitive values (e.g. identifiers) cannot be <i>seen</i> or <i>reasonably recovered</i> in the event of a compromise.
Illustrative Example:	Suppose a malicious actor manages to extract a database which stores passwords. By applying “hashing with salt” to the passwords, the malicious actor would not be able to see the original password, and <u>has no reasonable way to recover the original password.</u>

	 <p>Nevertheless, it is still possible to authenticate passwords by applying this hashing function with the correct salt value on the password inputted and comparing the hashed values.</p>
<p>Technical Implementation:</p>	<p>Replace sensitive values (e.g. identifiers) with an algorithmically derived value that <u>cannot be reversed easily</u>.</p>
<p>Additional Remarks:</p>	<p>This measure is appropriate for data fields where the actual values need not be recovered, such as passwords or for aggregated data analytics.</p> <p>Strong hashing functions should be used, such as cryptographic hash function, that cannot be reversed with current computing resources.</p>


<p>Measure:</p>	<p>T8. Field-level encryption</p>
<p>Purpose:</p>	<p>Ensure that sensitive values cannot be <i>seen</i> in the event of a compromise.</p>
<p>Illustrative Example:</p>	<p>Suppose a malicious actor manages to extract a database which stores income. Unless the malicious actor manages to obtain the <i>secret key</i>, he would not be able to see the original value (income).</p>  <p>Authorised users can restore the true value with the correct secret key.</p>
<p>Technical Implementation:</p>	<p>Encrypting specific data fields to hide the true value. A different secret encryption key is to be used for each field.</p>
<p>Additional Remarks:</p>	<p>The underlying technique of field-level encryption achieves the same function as “T9. Tokenisation”.</p> <p>The technical implementation of field-level encryption uses a <i>mathematical encryption function</i> instead of a <i>lookup table</i> for tokenisation. Field-level encryption is more appropriate where the actual values need to be frequently recovered.</p>

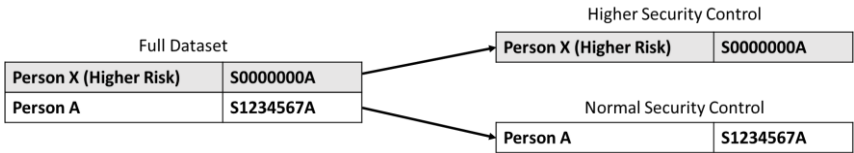
Measure:	T9. Tokenisation
Purpose:	Ensure that identifiers cannot be <i>seen</i> in the event of a compromise.
Illustrative Example:	<p>Suppose a malicious actor manages to extract a database which stores NRICs. Unless the malicious actor manages to obtain the <i>lookup table</i> (i.e. the full mapping of values to <i>tokens</i>), he would not be able to see the original NRIC.</p>  <p>Authorised users are able to restore the true value with the correct token.</p>
Technical Implementation:	Replace identifiers and attributes with a different value known only to the agency.
Additional Remarks:	<p>The underlying technique of tokenisation achieves the same function as “T8. Field Level Encryption”.</p> <p>This technique is appropriate for data fields where the actual values need to be recovered, such as identifiers required for service delivery.</p>

Measure:	P8. Manage keys to data protection technical safeguards
Purpose:	Ensure the effectiveness of the technical safeguards of tokenisation and field-level encryption by keeping the “key” safe.
Illustrative Example:	Suppose the officer is using a set of tokenised data for analytics purposes. He/she will be unable to re-identify the individuals, as there are processes to ensure that the officer holding the key is not the same person as the officer using the data.

12 **Partially hide the full data.** This ensures that even if an attacker were to break into the IT system, the damage would be limited as he/she would have no access to the full data.

Measure:	T10. Obfuscation/ masking/ removal of entity attributes
Purpose:	Ensure that the exact sensitive values cannot be <i>seen</i> or <i>ever recovered</i> in the event of a compromise, although approximate or noisy values might still be seen.

<p>Illustrative Example:</p>	<p>Suppose an agency wishes to send customer service agents some credit card numbers for verification purposes. They might mask the first 12 digits before sending it over, as the last 4 digits are sufficient for verification.</p> 
<p>Technical Implementation:</p>	<p>Hide the true value of the attributes by adding noise, banding the data, or masking out portions of the value. Attributes not relevant for data usage should be removed.</p>
<p>Additional Remarks:</p>	<p>This measure is appropriate where the exact values are sensitive, but noisy values (that are less sensitive) are sufficient for usage and exploitation.</p>

<p>Measure:</p>	<p>T11. Dataset partitioning (of entities or attributes)</p>
<p>Purpose:</p>	<p>Ensure that information on selected entities or attributes will not be compromised even if the larger database has been compromised. This could include individuals in vulnerable positions or sensitive attributes.</p>
<p>Illustrative Example:</p>	<p><u>Example 1: Dataset partitioning of vulnerable individuals</u> Suppose the database of all citizens is compromised. Personal data on vulnerable individuals will also be compromised as part of the larger dataset compromise. By partitioning out vulnerable individuals, the database leak would not include these individuals. Agencies can apply higher security controls to the separate database consisting of vulnerable individuals.</p>  <p><u>Example 2: Dataset partitioning of sensitive attributes</u> Suppose a database containing details of persons is compromised. Sensitive attributes of these persons will also be compromised as part of the larger dataset compromise. By partitioning out sensitive attributes, the database leak would not include these attributes.</p>

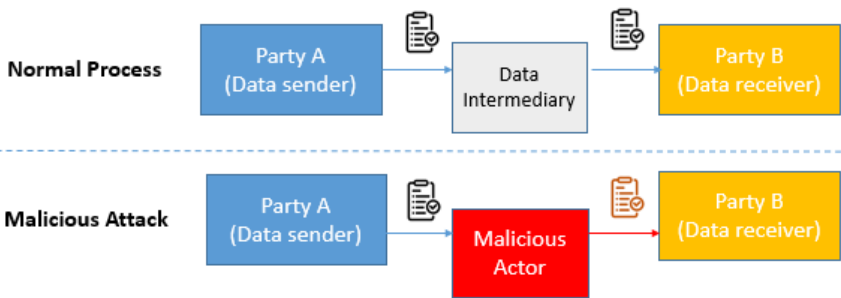
Technical Implementation:	<p>Break a dataset into smaller datasets by segmenting out selected entities or attributes and apply different access controls to each of the partitions.</p> <p>The partitioning of the dataset can be achieved by either: (a) physically partitioning of the dataset in different storage locations; or (b) virtually partitioning of the datasets in different virtually isolated partitions. Each dataset partition, physical or virtual, would have different access controls.</p>

13 Protect the data during distribution. Another common source of data incidents is when a public officer mistakenly distributes the data file to unauthorised parties, for example, via email. An unauthorised party could also intercept the data during transit. Data must therefore be protected during the distribution phase as well.

Measure:	T12. Password protecting and encrypting files
Purpose:	Ensure that only the <i>receiver</i> with the password can access the file.
Illustrative Example:	Suppose that an officer accidentally sends an Excel file with sensitive personal data to an unintended recipient X. Without the password, recipient X will not have access to the data in the Excel file.
Technical Implementation:	Secure a file using encryption and password such that only authorised users can access and change the content.

Measure:	P9. Securely distribute passwords out-of-band
Purpose:	Ensure the effectiveness of the technical safeguards of password protecting and encrypting files.
Illustrative Example:	Suppose an officer accidentally sends a password-protected file to the wrong party. If the password was sent together with the email, the unauthorised party would have access to the underlying dataset. This measure ensures that the password

	is transmitted through a different channel, such as through text or call or trusted Instant Messaging services.
--	-----------------------------------------------------------------------------------------------------------------

Measure:	T13. Data file integrity verification
Purpose:	Ensure that the <i>receiver</i> gets the same file that the <i>original sender</i> intended.
Illustrative Example:	<p>Suppose that Party A sends sensitive data to Party B through a data intermediary. A malicious actor playing the role of the intermediary might modify the dataset and send the modified file to Party B. This might cause severe disruptions to operations and service delivery, even though the underlying database has not been modified.</p>  <p>This measure allows Party B to verify that the data is the same as what Party A has sent, and protects such data against malicious attacks.</p>
Technical Implementation:	Original data sender provides a checksum or digital signature that confirms the integrity of a data file.

Measure:	P10. Distribute files through appropriate secure channels
Purpose:	Ensure that the distribution channels for sensitive files have the appropriate security safeguards.
Illustrative Example:	Suppose an officer wishes to send a sensitive entity dataset to another agency. The distribution channel that the officer uses should encrypt the file during transmission so that any attacker who maliciously intercepts the file would not be able to retrieve the original contents.

Recommendation 1.4: Develop and maintain expertise in advanced technical measures.

14 The Committee has identified 6 “advanced safeguards” to better protect data. These safeguards rely on emerging technology and techniques. These solutions might

not be mature enough for large-scale deployment or readily integrable within Government at the time of this report. The Government should monitor the development of these safeguards and deploy them when appropriate. Beyond these 6 advanced safeguards, the Government must put in place organisational structures and capabilities to continually identify, develop and deploy new technology that can further strengthen the public sector data security regime. This is covered under *Recommendation 5.2*.

15 Advanced safeguards to mitigate high-risk scenarios. For high-risk scenarios, the Government can consider deploying more advanced safeguards to mitigate the likelihood and impact of a data incident.

Measure:	A1. Homomorphic Encryption
Purpose:	Ensures that the data stays encrypted even during processing.
Illustrative Example:	Suppose that multiple agencies wish to send their respective data files to a data intermediary for fusion and processing. With homomorphic encryption, this data file can be fused and processed while staying encrypted. In this way, the data intermediary would not have access to any of the underlying datasets.

Measure:	A2. Multi-Party Authorisation
Purpose:	Mitigates the risk of a malicious insider trying to access the data file.
Illustrative Example:	Multi-party authorisation requires more than one password to unlock a sensitive file, analogous to multiple military officers are required to simultaneously launch the nuclear missile with their keys. Suppose that a malicious insider attempts to access a sensitive dataset. With multi-party authorisation, his password alone would not be sufficient to unlock the file.

16 Advanced anonymisation measures to enhance privacy. The Government should only give granular and exact data to officers where it is necessary for their use case. For data analytics purposes, it is often sufficient to gather the statistical characteristics of the data without having the exact data to re-identify the individual.

Measure:	A3. Differential Privacy
Purpose:	Ensures that the population level properties of the data set is still useful for analytics purposes while hiding preserving the privacy of the individuals in the dataset.
Illustrative Example:	Suppose that an officer wishes to perform data analytics and Machine Learning, and wishes to use the statistical characteristics of the dataset such as the average value. The

	officer will be able to do it, even without accessing the true value of each data item.
--	-----------------------------------------------------------------------------------------

Measure:	A4. Dynamic data obfuscation and masking
Purpose:	Ensure that the data can be obfuscated in different ways during processing so that the amount of obfuscation can be tailored for different access levels and different use cases.
Illustrative Example:	<p>Suppose the original addresses are stored in a database and the addresses are extracted for two different use cases: (a) verification of postal code for lucky draw; and (b) data analytics aggregated at the building level. With dynamic data obfuscation and masking, the different level of masking can be applied to the when the addresses are extracted out from the database for each of the use cases and the obfuscated addresses reveal only the appropriate amount of details.</p>

17 Advanced data distribution safeguards to protect data files directly. As Government files often move out of the secured, trusted Government network, the data protection measures are to be applied at the file level. The following safeguards provide an additional layer of protection at the file level:

Measure:	A5. Digital Signing of Data File
Purpose:	Verifies the originator and the content of the data file to ensure the integrity of the file.
Remarks	This safeguard requires the setting up of a Public Key Infrastructure to manage the digital certificates. While this safeguard achieves the same outcome as both the data file integrity verification and the digital watermarking of data files combined, it does so more efficiently.

Measure:	A6. Secured File Formats
Purpose:	Ensures that safeguards are applied at the file level so that these safeguards are still effective even outside the Government network.

Remarks	Suppose that an agency must pass a data file to a third party vendor. Secured File Formats allow finer control over what can be done to the data inside the file, even though it is outside the Government network. This includes controlling whether the content can be copied or modified, and tracking whether the file has been accessed, transferred or downloaded.
---------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Implementation of technical and process measures using a risk-based approach

18 The technical and process measures should be implemented using a risk-based approach. Each agency will use a common Whole-of-Government data security risk assessment matrix to determine the risk level of their data. The agency would select the relevant technical measures that would enable them to manage their risks appropriately. For example, systems containing highly-sensitive data that is widely accessed by authorised users should incorporate the measures that provide the highest levels of protection such as hashing-with-salt, tokenisation or field-level encryption. The agency would also have to take into account its operational context when deciding on the measures to implement. For example, hashing-with-salt irreversibly changes a data field; it would be suitable for use in analytics systems where only de-identified data is required, but not appropriate for use in operational systems which require identifiable data for service delivery.

Recommendation 1.5: Enhance the data security audit framework to detect gaps in practices and policies before they manifest into incidents.

19 The Committee notes that the Government audits agencies' compliance with data security policies, as part of a broader audit on compliance with all Government IT policies. Based on the learning points from the inspections of data management practices, the Committee recommends enhancing the Government's data security audit and monitoring framework in the following ways:

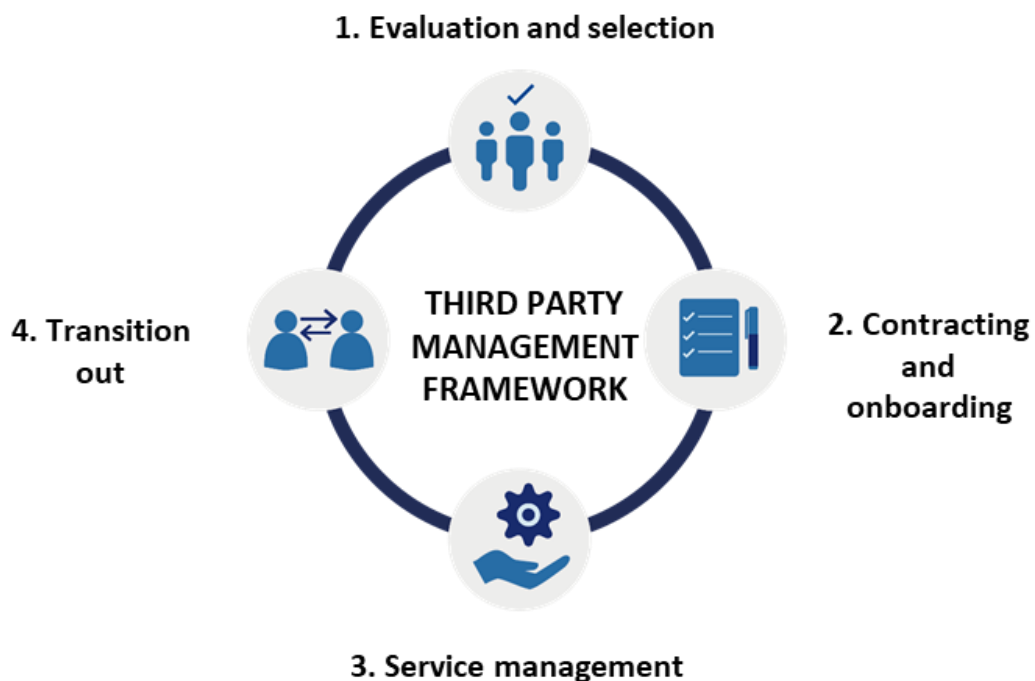
- a. **Enhance the coverage of data security risks.** In practice, data incidents are not confined to a single system, as data is often shared between systems and there are people and process risk factors that are not limited to a technical system. Audits should therefore focus on whether the data is well secured throughout its lifecycle, rather than merely whether the system has incorporated the appropriate safeguards.
- b. **Adopt a risk-based approach.** Agencies should continue to be scheduled for audits at least once in 3 years, with higher-risk agencies being audited more frequently. Risk will be determined based on the data/system's security classification and Information Sensitivity Framework (ISF) categorisation. These centrally-led audits will be complemented by agency-driven audits on lower-risk systems to ensure that all systems are adequately covered.
- c. **Focus on the effectiveness of safeguards besides compliance with policies.** Currently, data security audits focus primarily on whether

centrally-mandated policies are complied with, rather than whether the safeguards are actually effective. The Committee recommends that the audits incorporate tests to determine the effectiveness of the agency's technical and process controls. The duration of the audits should also be extended from four to six weeks, in view of the expansion of the audit scope.

Recommendation 1.6: Enhance the third party management framework to ensure that third parties handle Government data with the appropriate protection.

20 The Committee recognises that public agencies work extensively with third parties to deliver services to citizens, carry out operational functions, and provide consultation services for policy analysis and planning. When doing so, these third parties may handle large volumes of Government data. The high standards of data protection that the Government places on itself must also extend to these third parties.

21 The Committee recommends that the Government set out a third party management framework to guide agencies in ensuring that third parties protect Government data well. The proposed framework is built around the various stages of the third-party project life-cycle. It includes requirements for agencies to assess the risk of assigning a work to a third party, implement the necessary policies, establish a governance structure to monitor the third party's performance and an audit regime to verify the third party's compliance with stated policies.



22 The key elements of the enhanced Third Party Management Framework are as follows:

Stage 1: Evaluation and Selection

23 Agencies will be required to identify, assess, prioritise and mitigate the risks identified in outsourcing work to the third party, to manage the data security and operational risks to the Government.

Stage 2: Contracting and Onboarding

24 Agencies will be required to incorporate the relevant terms and conditions including data security and governance requirements into the contracts or equivalent instruments with third parties.

25 Agencies will also be required to conduct a competency assessment, obtain the necessary security clearance and carry out on-boarding briefings (with annual refresher) for third parties. This ensures that third parties are cleared and equipped to carry out the assigned work according to the Government and Agency-specific ICT and Data management policies.

Stage 3: Service Management

26 Agencies will be required to maintain a registry of work assigned to third parties. The registry will include the third party's roles and responsibilities, the data collected, stored and processed by the third party and also the assets and equipment assigned to the third party.

27 Agencies will be required to establish a governance structure to monitor and review the third party's performance, and compliance of the third party with applicable Government policies and standards defined in the contractual or equivalent instruments.

28 Agencies will be required to perform regular checks, including annual self-assessment or/and audits, on the third party to determine the third party's level of compliance (set out in paragraph 27). The third party audit regime is premised on a risk-based approach, with more stringent requirements imposed on third parties dealing with higher-risk systems. The audit scope and frequency, and the need for an independent auditor, will be guided by the risk assessment based on the system's security classification and sensitivity categorisation according to the ISF.

Stage 4: Transition Out

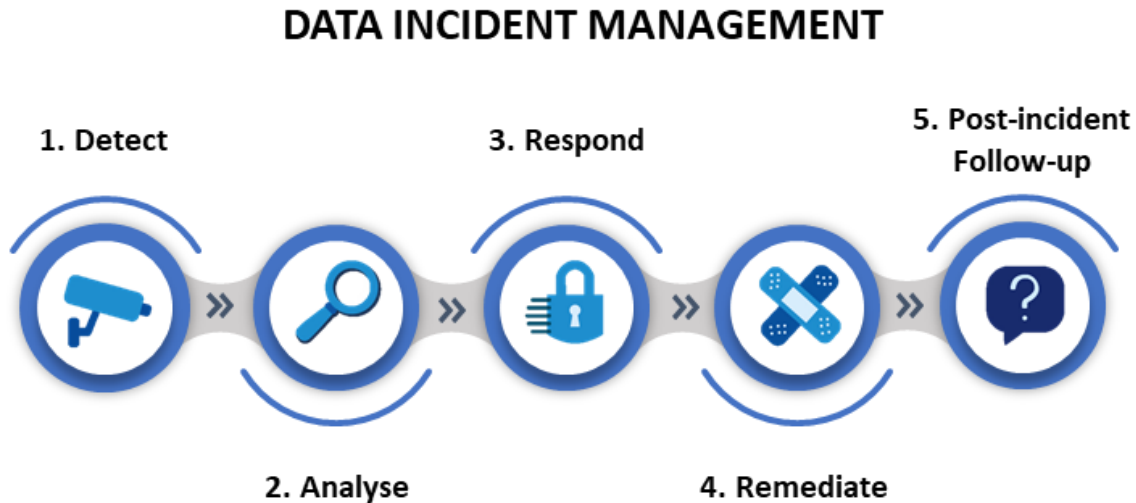
29 Agencies will be required to develop and maintain up-to-date exit management plans. This ensures that upon the termination of third party services, there will be no disruption of services, data would be appropriately returned and/or destroyed and the necessary expertise and security posture will continue to be maintained. Agencies must also conduct exit checks and audits before the third party discontinues its services. The need for an independent auditor to conduct the third party's exit audit will depend on the risk assessment.

ANNEX D: KEY RECOMMENDATION 2 - ENHANCED DATA INCIDENT MANAGEMENT FRAMEWORK

Strengthen processes to detect and respond to data incidents swiftly and effectively

1 While the Government implements preventive measures to facilitate the secure usage and sharing of data, it must remain vigilant and be well-prepared to detect and respond swiftly and effectively when there are data incidents.

2 The Committee's recommendations are structured around the five-stage operating procedure in managing data incidents of "Detect", "Analyse", "Respond", "Remedy" and "Post-incident Inquiry". The first stage is to **detect** and confirm an incident through active logging and monitoring, or through reports from the public or other public agencies. The second stage is to **analyse** the facts and evidence to determine how to respond to the incident. At this point, the Police will be alerted if there is prima facie evidence of a crime having been committed. The third stage is to **respond** to the incident by containing the damage through eliminating vulnerabilities, working with other agencies where necessary. The fourth stage is to **remediate** by restoring systems to an operationally ready state and to engage affected parties. Finally, the last stage is to undergo a **post-incident follow-up**, in order to understand the root cause of the incident and recommend ways to prevent a similar incident from occurring.



Stage 1: Detect

- 3 There are several ways to detect a data incident:
- a. *Active monitoring of log files and network traffic to identify anomalous behaviour and potentially malicious activities.* The Government currently has processes in place to do this. The Committee's recommendation to implement measures to "T4. Enhance Logging and Monitoring" would further bolster the Government's capabilities in this area.

- b. *Reports from public officers and members of the public.* Currently, all public officers are required to report data incidents that they might have committed or discovered (e.g. when an officer inadvertently sends an email with sensitive data to the wrong recipient).

However, there is no established central point for a member of the public to lodge a complaint about a data incident. This could lead to delays in incident response and inefficiencies in complaint resolution as members of the public may not know who they should lodge a complaint with. This is particularly so if they do not wish to complain to the affected public agency and prefer an independent party to look into the complaint.

Recommendation 2.1: Establish a central contact point in the Government Data Office to which the public can report Government data incidents. This complements the current processes for agencies to report Government data incidents to the Smart Nation and Digital Government Group (SNDGG).

4 The central contact point will minimise confusion on where the public may lodge complaints on Government data incidents, and assure the public that an authoritative independent party would follow up on the complaint. Having a central contact point would ensure greater consistency in the handling of data incidents across agencies. The Committee recommends establishing the central contact point in the Government Data Office (GDO). It should have close links with the Government Technology Agency of Singapore (GovTech) and partner agencies such as the Cyber Security Agency (CSA) for cybersecurity-related incidents and the Personal Data Protection Commission (PDPC). In the early stages of the incident, the facts of the case may not be clear and it may not be immediately apparent which public agency would be involved. Having strong links with partner agencies is therefore crucial to enable the quick triaging and assessment of the complaint.

Stage 2: Analyse

5 After detecting a data incident, agencies must gather evidence to establish the facts and causes of the incident. This is supported by technical measures such as *T3. Digital Watermarking of Files* to trace whom the dataset originated from and *T4. Enhanced Logging* of access to sensitive data so that investigators can find out how the data has been compromised and the person(s) involved in it.

6 After establishing the facts, public agencies will need to assess the severity of the incident⁵. This assessment would subsequently guide the response to the incident.

7 At present, this assessment is made by the agencies affected by the incident as they have the contextual knowledge to do so. While there are merits to this approach, it may lead to inconsistent assessments of impact and potentially inconsistent incident responses across agencies. For example, an individual agency may not give sufficient attention to incidents that could affect other agencies. Agencies

⁵ The severity of data incidents is assessed on a 5-point scale, based on impact to the affected individuals, organisations, public agencies and the State. The scale, in descending order of impact, runs as follows: Very Severe, Severe, High, Medium, and Low.

may also have different understanding of impact to individuals, which can lead to inconsistent approaches in notifying individuals affected by data incidents.

Recommendation 2.2: Designate the Government Data Office to monitor and analyse data incidents that pose significant harm to individuals. This ensures that large-scale incidents are escalated for timely and appropriate response.

8 The Committee recommends that the GDO monitors and analyses data incidents that pose significant harm to individuals, and escalates them to the appropriate platforms for response. GDO is best-placed to do this as it receives reports on all Government data incidents and is able to make an informed assessment of the impact of an incident relative to others. GDO should make its assessment based on the facts and inputs gathered from the affected agency and other public agencies, such as the CSA where Critical Information Infrastructures (CII) are concerned. GDO should assess whether the incident has wider implications on Government data security and whether the scale of the incident is significant. Where appropriate, GDO may submit a recommendation of the assessed impact for the relevant Minister's decision.

Stage 3: Respond

9 Following the analysis of the severity of the incident, the Government should contain the damage caused by the incident. This includes eliminating the underlying vulnerabilities that led to the incident, containing the scale of the incident, mitigating its effects and damage and resolving the incident. Where the data incident goes beyond the ambit of a single agency to manage or has severe impact on individuals or other agencies, a Whole-of-Government (WoG) effort will be required.

10 Today, there are established decision-making authorities within the Government for incidents classified as "Very Severe". However, for all other data security incidents, agencies handle the response on their own or escalate the incident on a case-by-case basis. This could lead to indecisiveness and delays in a WoG response, which could result in further damage to other Government systems.

Recommendation 2.3: Designate the Government IT Incident Management Committee as the central body to respond to large-scale/multi-agency incidents with Severe impact.

11 The Government IT Incident Management Committee (GITIMC) should determine the strategy to contain the impact of the incident on Government data and systems. This includes decisions on the allocation and use of Government IT resources, and the coordination of a multi-agency approach to respond to the incident, including the roles of key partner agencies such as the CSA, PDPC and the Police. The GITIMC should also formulate the broad strategy on the public communications of the technical aspects of the incident. The affected agency would remain accountable and responsible for the operational aspects of managing the incident, as the agency would know the systems, data and affected individuals best.

Stage 4: Remediate

12 After the threat has been eradicated, remedial actions must be taken. This includes restoring systems to an operationally-ready state and notifying individuals affected by the data incident. The latter must be done in a timely and effective manner to enable affected individuals to take the necessary steps to prevent further damage to themselves. Today, notification of affected individuals is initiated by agencies on a case-by-case basis, although GDO provides guidance to agencies upon request for advice.

Recommendation 2.4: Institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact to the individual.

13 Under this framework, agencies must notify all affected individuals when the data incident is likely to result in significant harm or impact to the individuals. The only exception to this is when notification would affect the public interest, such as a compromise of national security or national interests, or ongoing investigations by an agency authorised by law. This adopts the same approach as the PDPC's proposed mandatory notification of individuals affected by data breaches⁶.

14 The main elements of the Government's notification framework, which are the same as those in PDPC's proposed mandatory breach regime, are captured in the table below:

1. Definition of a "data incident"	An incident exposing personal data in an organisation's possession or under its control to risk of unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks.
2. Criteria for notifying affected individuals	When an incident is likely to result in significant harm or impact to individuals to whom the information relates.
3. Contents of notification	<ul style="list-style-type: none"> a. How and when the data incident occurred b. Types of personal data involved in the data incident; c. What the agency has done or will be doing in response to the risks brought about by the data incident; d. Specific facts on the data incident where applicable, and actions individuals can take to prevent that data from being misused or abused; e. Contact details and how affected individuals can reach the agency for further information or assistance (e.g. helpline numbers, e-mail addresses or websites); and/or f. Where applicable, what type of harm/impact the individual may suffer from the compromised data.

⁶ The PDPC intends to introduce a mandatory data breach notification regime as part of the PDPA review in 2020. When there is significant harm or impact to individuals affected by a data breach, organisations will be required to notify them.

4. Modes of Notification	<p>GDO will work with the affected agency to determine the best way of notifying affected individuals.</p> <p>Agencies should adopt the most effective way to reach out to individuals, depending on the urgency of the situation and number of individuals affected. These can include media releases, social media, e-mails, telephone calls, faxes and letters.</p>
5. Time Frame for Notification	<p>As soon as practicable.</p> <p>The final decision on notification should be made no later than 72 hours from the confirmation of the incident. Where agencies are not sure if they should notify the affected individuals, they should seek advice from GDO.</p>
6. Exceptions to Notification	<p>Where notification would cause harm to the public interest (including national security or national interests, or ongoing investigation of an agency authorised by law).</p>

15 Ensuring that individuals are able to take remedial action for a data incident sets the tone that the Government manages citizens' data with their interests in mind.

Stage 5: Post-incident Inquiry

16 Today, all data incidents undergo a post-incident inquiry. The affected agency undertakes the post-incident inquiries to understand the root cause of the incident and to identify ways to prevent a similar incident from occurring. Inquiries typically cover the effectiveness of the agency's data governance policies and practices, and evaluate the adequacy of the response actions taken.

Recommendation 2.5: Establish a standard process for post-incident inquiry for all data incidents. Inquiries into data incidents with at least significant public impact are to be conducted by parties independent of the affected agency.

17 There is currently no standard process on when post-incident inquiries should be undertaken by parties independent of the affected agency. Particularly for data incidents with significant impact on members of the public, agency-led inquiries may be perceived to lack independence, and the soundness of the inquiry outcome may be called into question.

18 The Committee thus recommends that all inquiries into incidents with at least significant public impact be conducted by a party independent of the affected agency (Independent Inquiry). These include incidents that cause death, serious consequences, or serious harm to members of the public.

19 For highly significant⁷ incidents, the Minister-in-charge of Public Sector Data Governance or the relevant Minister should convene a Committee of Inquiry (COI) to conduct an inquiry into these incidents. The composition and conduct of the COI would be guided by the Inquiries Act, and the findings of the COI would be made public. However, parts of the COI findings could be redacted if the published findings would adversely impact the public interest, for example, where it might compromise national security.

20 For significant incidents⁸, the Head of Civil Service (HCS) should commission an Independent Inquiry. This should be led by an individual who is not from the affected agency, with seniority at least equivalent to a Chief Executive or a Deputy Secretary. This could include public service leaders, retired public officers and non-Government experts.

21 Where the Minister-in-charge of Public Sector Data Governance or the relevant Minister considers it appropriate to do so, he may convene a COI or direct an Independent Inquiry to be commissioned for incidents that do not meet the threshold of “highly significant impact” or “significant impact”.

Recommendation 2.6: Distil and share learning points with all agencies to improve their data protection policies/measures and response to incidents.

22 The Committee recommends that all affected agencies submit their post-incident inquiry reports to GDO two weeks after completing the inquiry. The aim is to:

- a. Distil the learning points which are pertinent to the rest of the public sector and communicate them to the rest of the agencies;
- b. Review whether new or improved measures, processes and policies are required for the WoG; and
- c. Mandate and ensure compliance if there is a need for changes in WoG data security measures and practices.

⁷ A highly significant incident is one which:

- Causes the death of an individual
- Could cause public harm or endanger public safety or public health

⁸ A significant incident is one which could cause serious harm, including physical, financial or reputational, to an individual.

ANNEX E: KEY RECOMMENDATION 3 – MEASURES TO RAISE PUBLIC OFFICERS’ COMPETENCIES AND INCULCATE A CULTURE OF EXCELLENCE IN USING DATA SECURELY

Improve culture of excellence around sharing and using data securely, and raise public officers’ competencies in safeguarding data

1 While we implement sound technical and process safeguards, every public officer must play his/her role in safeguarding the data used. To this end:

- a. Public officers must be clear about their roles and responsibilities with regard to safeguarding data;
- b. Public officers must have the requisite capabilities to carry out those roles and responsibilities effectively;

2 These must be undergirded by a culture of excellence towards using data securely. A public officer who is only concerned about complying with a list of process and technical requirements will only be able to deal with threats of the past. He/she will not be well-prepared to identify and mitigate risks and emerging threats. He/she will need to move beyond compliance with baseline requirements to being sensitive to data security risks and proactively managing them.

3 The Committee’s recommendations target the following groups of public officers:

- a. Top leadership of public agencies;
- b. Key appointment holders, such as the Chief Data Officer, the Chief Information Security Officer and the Chief Information Officer;
- c. ICT (including cybersecurity teams) and Data teams; and
- d. All public officers.

Groups of Public Officers

The Committee’s recommendations are targeted at the following key groups of public officers:



Top Leadership



Key Appointment Holders



ICT, Cyber and Data Teams



All Public Officers

- Chief Data Officer
- Chief Information Security Officer
- Chief Information Officer

Recommendation 3.1: Clarify and specify the roles and responsibilities of key groups of public officers involved in the management of data security.

4 All officers must be clear about their roles in using data securely. Clear roles and responsibilities will inculcate a sense of ownership and accountability over data security. These roles and responsibilities should be set out in the IM8 PDM.

5 Each group of public officers plays complementary roles in building a strong data security regime:

- a. Top leadership** take command responsibility to strengthen their organisations' data security, and to develop a culture of excellence in using data securely. To ensure that their agencies use data securely, top leadership must:
- i. Combine operational know-how with data security principles, to apply data security well in the context of the agency's missions and operating environment
 - ii. Adopt holistic digitalisation strategy that promotes both data use and protection
 - iii. Monitor organisational performance in data security, e.g. through organisational KPIs
 - iv. Ensure that agency processes continually improve to adopt best practices

To inculcate a culture of excellence, top leadership must also:

- i. Build up officers' knowledge and confidence in handling data
- ii. Cultivate an open, learning environment where officers are vigilant and comfortable in reporting near-misses and data incidents
- iii. Develop a proactive organisational mindset of wanting to use data securely, rather than avoid data-driven approaches for fear of risks

- b. Key Appointment Holders** drive and monitor data security policies and measures:
- i. Chief Data Officer promotes the sharing and usage of data in a secure manner.
 - ii. Chief Information Security Officer ensures that the data in ICT systems and infrastructure are protected to a high level of security.
 - iii. Chief Information Officer drives the development and use of effective ICT systems and infrastructure to support agency functions.

The division in responsibilities of Key Appointment Holders encourages a healthy tension between data security, systems efficiency and data exploitation. Tension within the organisational structure is key as it acts as a 'check and balance' for competing objectives. For instance, there needs to be a balance between designing ICT systems and infrastructure that are efficient and effective for agency functions, and ensuring that there are a strong set of security measures built into the design of these systems.

- c. ICT, cyber and data teams** are directly responsible for data security within their respective systems and projects. This includes implementing and

managing the operations of data security measures, and regularly assessing their adequacy. They must also proactively detect and report incidents for their projects and systems, in accordance with the Standard Operating Procedures.

- d. **All public officers** are responsible for data security in their day-to-day work. This requires them to be aware of data security risks and consequences and maintain vigilance. Public officers must apply appropriate data security measures in their daily work and follow data security policies and processes. This includes proactively identifying and escalating data security incidents or non-compliance with these policies.

Recommendation 3.2: Equip these key groups with the requisite competencies and capabilities to perform their roles effectively.

6 In order to perform their roles in data security effectively, public officers must build up their data security competencies. Training should be done regularly so that their competencies stay relevant in a constantly changing environment. Training options range from basic data security awareness for all public officers, to specialised technical training for ICT, cyber and data Teams.

7 Today, all public officers are required to attend the IT Security Awareness course on an annual basis, which raises public officers' baseline level of cybersecurity awareness. However, there is no equivalent module for data security. **The Committee recommends that all public officers complete a module on data security** to equip them with a baseline level of awareness and understanding of data security risk, and the policies and practices that address them such as the process safeguards recommended by the Committee. This data security module should be made **mandatory for all public officers to attend on an annual basis**. In addition, **public officers should provide an annual declaration** to attest that they are aware of their responsibilities and liabilities in handling Government data and reinforce their commitment to data security.

8 Public officers should also be required to attend training courses tailored according to their roles and responsibilities. **ICT, cyber and data teams should attend technical training focused on data protection solutions** (such as data anonymisation, database management) as they are directly responsible for implementing data security measures. The Committee recommends that the Government regularly update the training requirements and courses available for each group of officers.

9 Besides formal training, the Committee recommends that the Government form **a Community of Practice comprising Data Security Practitioners across all public agencies**. This forum will enable members to share good practices and lessons learnt from past data incidents and near misses. The collective knowledge and experiences shared could help to minimise recurrence of data incidents.

Recommendation 3.3: Inculcate a culture of excellence around sharing and using data securely.

10 In order to build a strong and robust data security regime, it is imperative that public officers move from a compliance-based system to one that aims to achieve excellence. A compliance-based approach, which involves ticking off a checklist of requirements, is useful. However, such a list would always be one step behind, as meeting the requirements would only address threats of the past, not those of the future. The Government should move beyond an approach that only requires the achievement of a minimum threshold to one that encourages the pursuit of excellence. This should be embedded within the ethos of the public service and the culture of each agency, and carried by all public service officers.

11 Fundamentally changing the culture of an organisation is not an easy feat, especially for a large organisation like the Public Service. This will require sustained efforts across many years at all levels of the organisation. Top Leadership and Key Appointment Holders must set the tone from the top and lead these efforts by rewarding and encouraging good data security practices, and consistently reiterating key data security messages.

12 The Committee recommends that the Government work towards developing a culture of open reporting of all types of data incidents (whether major or minor ones) as well as confirmed incidents and “near-misses”. This would achieve two desirable outcomes. First, agencies would be alerted to potential data incidents in a timely manner. This enables agencies to take active steps to respond to the incident and contain the impact of the incident. Second, the reporting of near misses enables agencies to identify and rectify problems in their data security policies and practices before they lead to actual data incidents.

13 To inculcate a culture of open reporting, Top Leadership and Key Appointment holders must create an environment where all officers are comfortable and motivated to flag out potential gaps in our data security regime or suspected data incidents. The focus should be on learning from potential mistakes, rather than on assigning blame or imposing punishment on culpable individuals.

ANNEX F: KEY RECOMMENDATION 4 – MEASURES TO IMPROVE ACCOUNTABILITY AND TRANSPARENCY

Enhance frameworks and processes to improve accountability and transparency of public sector data security regime

1 All public agencies and public officers must uphold high standards to protect Government data. There are existing accountability frameworks and legislative measures to hold leaders and individuals accountable for all issues under their purview, including data protection.

Box F1: Accountability for Data Protection in the Public and Private Sectors

In the public sector, the Government prescribes punitive measures to be taken against public officers involved in data incidents. These include

- a. Criminal penalties of fines up to \$5,000 and/or up to 2 years' imprisonment for the following acts prescribed in the PSGA:
 - i. Reckless or intentional disclosure of data without authorisation.
 - ii. Improper use of data for a gain.
 - iii. Reckless or intentional attempt to re-identify anonymised data.
- b. Disciplinary measures set out in the Public Service (Disciplinary Proceedings) and administrative measures set out in the Public Service Division's accountability frameworks. These measures include:
 - i. Counselling, warnings or reprimands;
 - ii. Stoppage of increment, fines, adjustments in bonus payments;
 - iii. Re-deployment, reduction in rank, retirement, dismissal.

The Government does not impose financial penalties on public agencies as monies that fund financial penalties would come from the same public purse. Such a practice could adversely affect the public agency's ability to operate or deliver services to citizens.

Under the PDPA, private sector organisations are accountable for the management of personal data under their possession or control. Where a private sector organisation fails to take the necessary steps to protect personal data, PDPC can take enforcement action including issuing directions to the organisation to rectify the problem and imposing financial penalties of up to \$1million. Organisations are liable for the actions of their employees acting in the course of their employment with the organisations. The relevant organisation would have the discretion to decide how it wishes to take disciplinary action against its employee for data management lapses.

2 The Committee recommends augmenting the existing accountability and disciplinary frameworks with initiatives to strengthen data security as an organisational and leadership priority. The emphasis on data security should grow in tandem with public agencies' strategic push to share and use data more widely for citizens' benefit.

Recommendation 4.1: Institute organisational Key Performance Indicators (KPIs) for data security to signal data security as an organisational priority and for leaders to be responsible for performance.

3 Currently, some public agencies have instituted organisational KPIs on data security (e.g. number of data incidents, classified by severity). However, this is not a standard practice across the public sector. The Committee recommends **introducing organisational KPIs on data security to elevate data security as an organisational and leadership priority**. This will enable the organisation and its leaders to monitor how well data is protected and the effectiveness of its response to data incidents.

4 Top Leadership should monitor these KPIs and report them to their Boards of Directors and/or the proposed WoG Committee overseeing data security (see Recommendation 5.1).

5 Examples of such KPIs, adapted from security frameworks and industry best practices, include:

- a. Proportion of officers trained in a data security annually
- b. Outcome of data security audits (based on broader IM8 audit results)
- c. No. of data incidents assessed as Severe or Very Severe in a year
- d. Average time taken between detection and resolution of a data incident
- e. Average time taken to notify individuals affected by a data incident

Recommendation 4.2: Mandate that the top leadership of all public sector organisations be accountable for putting in place a strong organisational data security regime.

6 The Committee recommends making clear that Public Service Leaders are responsible for implementing appropriate processes and measures to ensure that organisations have strong and resilient data security regimes. Leaders are accountable to their Boards of Directors and/or to the proposed WoG Committee overseeing data security (see Recommendation 5.1), similar to the way they are accountable for other governance issues such as HR and finance.

7 Leaders will be held accountable under the existing leadership accountability frameworks, if necessary data policies and processes are not implemented or are executed poorly due to management lapses.

8 The Committee suggests several ways in which leaders can strengthen their oversight over data security:

- a. Establishing organisational platforms to discuss data security at the top management level
- b. Reviewing the organisation's data security posture and readiness regularly
- c. Monitoring data security KPIs to understand their organisation's data security performance (see Recommendation 4.1).

Recommendation 4.3: Make the impact and consequences of data security breaches salient to public officers.

9 The Government has a comprehensive disciplinary framework for public officers and laws (e.g. PSGA) to hold individuals accountable for data incidents. However, the Committee observed that public officers generally lack awareness of the impact and consequences of data incidents.

10 The Committee recommends that the Government raise public officers' awareness of the adverse impact of failing to protect data, particularly on:

- a. The privacy of the individual or business to whom the data relates;
- b. The Government's and their organisation's ability to function effectively; and
- c. The consequences that the individual might face for his part in the data lapse. For leaders, this should include how the leadership accountability frameworks apply to management lapses that result in ineffective data security policies/practices or data incidents.

11 The Committee recommends including such content in the:

- a. Planned mandatory data security course for all public officers; and
- b. The proposed Post-Course Declaration that all officers will sign at the end of the course in (a).

(See Recommendation 3.2 for the Committee's recommendations on (a) and (b).)

Recommendation 4.4: Ensure accountability of third parties handling Government data.

- a. **Amend the PDPA to ensure its scope covers agents of Government**
- b. **Amend the PDPA to bring non-Public Officers to task for recklessly or intentionally mishandling any personal data.**

12 The high standards of data protection that the Government imposes on itself should also extend to non-Government Entities and non-Public Officers who handle Government data, particularly personal data. These third parties should also be held accountable for data lapses that are directly or indirectly caused by their actions.

Non-Government Entities that Act on Behalf of Public Agencies

13 Currently, non-Government Entities are subject to the PDPA. However, they are excluded from the application of the data protection obligations in the PDPA when they are specifically authorised by a public agency to act on its behalf as its agent (agents of Government). Such authorisation is usually made expressly, for example through the terms of a contract. The PSGA does not cover such organisations as it focusses on the governance of public agencies. Hence, agents of Government are subject to the obligations in their contracts with public agencies and, where applicable, laws such as the Official Secrets Act. This legislative gap could undermine the security of Government data as agents of Government may handle large volumes of Government data.

14 To close this gap, **the Committee recommends that the PDPA be amended so that the PDPA covers all non-Government Entities, including agents of Government.** This will ensure that non-Government Entities are always covered under the PDPA with respect to their data protection practices.

Non-Public Officers' Accountability for Personal Data

15 Currently, both the PDPA and the PSGA do not cover non-Public Officers⁹ who recklessly or intentionally mishandle Government data, except for employees of contractors of the Government who misuse Government data for a gain.

16 Legislation (e.g. Official Secrets Act, Computer Misuse Act) and the common law action for breach of confidence that can be used to hold non-Public Officers accountable for unauthorised access or disclosure of data. However, these instruments serve purposes other than data protection (e.g. the Official Secrets Act focuses on protecting national security rather than protecting personal data) and do not cover the full array of data incidents that may occur. This could undermine the Government's ability to take non-Public Officers to task when data incidents occur.

17 The Committee recommends that non-Public Officers be held accountable for reckless or intentional mishandling of personal data, regardless of whether the personal data is from the public sector. Doing so would enhance the protection of personal data in Singapore against such misconduct.

18 The Committee therefore recommends **amending the PDPA to hold non-Public Officers accountable for egregious mishandling of personal data regardless of whether the data is from the public sector.** This is similar to how the PSGA holds public officers accountable for egregious mishandling of Government data. Such individuals should be liable for criminal penalties similar to those under the PSGA, if they are found to have done the following without authorisation:

- a. Recklessly or intentionally disclosed personal data;
- b. Intentionally used personal data for a wrongful gain or a wrongful loss to any person; or
- c. Recklessly or intentionally re-identified anonymised data.

19 The PDPA does not cover non-personal data, e.g. data about a business. Non-Public Officers will be held accountable for protecting non-personal data by way of contractual obligations and common law (e.g. common law duty of confidentiality). Non-Government Entities are held accountable for the protection of non-personal data in the same way today.

Transparency of the Government's personal data protection policies

20 The Committee notes that the PSGA and the IM8 PDM set out high data protection standards for the Government. However, the Government does not publish the IM8 PDM in the public domain. Citizens do not have information on the policies and standards that are imposed on the Government to protect their data, and how

⁹ This includes employees of Government contractors, independent researchers and members of the public.

effectively these have been implemented. The Committee recommends providing the public with more information about the Government's personal data protection policies and standards, and its data protection efforts.

Recommendation 4.5: Publish the Government's policies and standards on personal data protection

21 The Committee recommends that the Government publishes its policies and standards on personal data protection. This would allow the public to better understand how the Government's approach to personal data protection.

Recommendation 4.6: Publish an annual update on the Government's personal data protection efforts

22 The Committee recommends that the Government provides annual updates on its personal data protection efforts to provide public with visibility over the Government's efforts. The update should include how the Government keeps its data protection policies relevant and how its policies and standards have been implemented. The Committee suggests that this could be part of a broader update on personal data protection in Singapore, covering both the public and private sectors. The report should take into account Singapore's unique operating context, for example, its data-sharing efforts, its data protection/governance landscape.

- 23 The Committee recommends that the Government do this in two stages:
- a. (*Near-term*) Publish an annual report on its data security efforts in the year of concern, including learning points from past data incidents, new initiatives, implementation of measures (e.g. roll-out of technical measures), emerging data security risks and insights from opinion pieces.
 - b. (*Medium-term*) Develop comparative measurements or indicators that show the effectiveness of the Government's data security efforts, with a view to publishing such indicators in the aforementioned annual report.

ANNEX G: KEY RECOMMENDATION 5 – ORGANISATIONAL AND GOVERNANCE STRUCTURES

Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs.

- 1 The Committee is of the view that strong WoG organisational structures with the right mandate and resources are required to:
 - a. Implement the recommendations made by the Committee in an effective and timely fashion; and
 - b. Set in place structures and enablers to ensure that data security efforts are sustained in the long-run.
- 2 The Committee's recommendations are intended to ensure that its efforts to improve the public sector data security regime would not be once-off, but would be institutionalised through WoG structures.
- 3 The key data security functions are:
 - a. **Policy-making:** Set strategic direction and policies to identify, manage and respond to key data security risks
 - b. **Compliance assurance:** Ensure that agencies comply with the stipulated data security policies
 - c. **Capability-building:** Developing WoG data security capabilities and equipping each officer with the right competencies to use data securely
 - d. **Operations management:** Monitor and detect data security threats and incidents
- 4 Although there are existing parties within the Government overseeing the key functions, responsibility for such functions is currently diffused.
- 5 The Committee identified 3 gaps in the current WoG structures:
 - a. **Lack of high-level attention on data security at the WoG-level** – Data security may not be sufficiently discussed as a strategic consideration;
 - b. **Lack of a dedicated body to drive and coordinate data security efforts across the Government** – Potential lack of coherence and duplication in data security efforts; and
 - c. **Lack of a structure to deepen capabilities in data privacy protection technologies** – the Government's ability to safeguard data may not keep up with its ambitions to use data more widely to serve citizens better.
- 6 To address the three gaps identified, the Committee has made three recommendations:

Recommendation 5.1: Appoint the Digital Government Executive Committee, which is chaired by a Permanent Secretary as the high-level WoG body to oversee public sector data security and drive the implementation of the Committee's recommendations.

7 As the Government shares and uses data more pervasively, more attention needs to be devoted at the strategic level to ensure this is done in a secured manner. Currently, there are existing WoG committees that provide high-level strategic direction to the Government on digitalisation and data strategies. However, these committees do not oversee data security. As the use of technology and data advances, it is timely to appoint a high-level committee to ensure data security features more prominently in the WoG agenda.

8 The Committee recommends the **appointment of the Digital Government Executive Committee (“DG Exco”) as the WoG Committee to oversee public sector data security, alongside other ICT security matters.** The DG Exco currently provides strategic direction for WoG ICT&SS policies to raise the performance, security, and inter-operability of ICT&SS systems.

9 The Committee proposes that DG Exco's mandate be expanded to include data security. The DG Exco will provide strategic direction to ensure the Government's data security regime is kept up-to-date and evolve with changes in security threats and the use of data. This includes:

- a. Monitoring the progress of the implementation the Committee's recommendations;
- b. Monitoring the Government's data security landscape and readiness:
 - (i) Overall assessment of data security risks (informed by external scanning and audit findings) and ensure high risk systems are adequately protected
 - (ii) Monitor agencies data security performance (e.g. by creating a data security balanced scorecard); and
- c. Providing direction on data security policies and practices.

Recommendation 5.2: Set up a Government Data Security Unit to drive data security efforts across the Government.

10 Currently, WoG data security functions exist but they operate in separate units across the Government. A clearer organisational mandate is needed to drive and coordinate data security efforts across the Government is needed.

11 The Committee proposes the **establishment of a Government Data Security Unit (GDSU) to drive data security efforts across the public sector.** This will signal the Government's commitment in safeguarding data and driving data security across the Government.

12 The GDSU will drive the formulation of data security policies and risk mitigation initiatives, and the building of agencies' capabilities in data security. GDSU will be mandated and resourced to:

- a. Develop strategies to manage public sector data security, including identifying, assessing and prioritising risks, crafting new strategies and formulating new initiatives to mitigate risks and improve Government's response to data security incidents;
- b. Engage agencies on data security matters, and build agencies' capabilities in data security; and
- c. Lead on data privacy issues and examine the impact of Government data related policies and issues on individuals.

13 The GDSU should be sited within the GDO to build on and consolidate GDO's existing work in data security, and to enable GDO to drive data security as an enabler for data sharing and usage. This ensures that the Government adopts a security-by-design approach in its data sharing and management policies and initiatives (e.g. designing the Government Data Architecture to be the foundation of both data-sharing and data security).

Recommendation 5.3: Deepen the Government's expertise in data privacy protection technologies through GovTech's Capability Centres.

14 The Committee recommends that the **Government develop strong capabilities in data privacy protection technologies**. The frontier for data privacy protection technology is rapidly shifting. The Government should have the organisational capacity to develop and deploy emerging data privacy protection technologies so that it can maintain data privacy while enabling data to be used. The Committee recommends that the Government **deepen its expertise in data privacy protection technologies through expanding the scope of GovTech's Capability Centres**.

- 15 GovTech will:
- a. Develop the Government's capabilities in data privacy protection technology – both within the Centre of Government and in Agencies;
 - b. Recommend and develop data privacy protection technologies; and
 - c. Develop and implement solutions to preserve the confidentiality of data while enabling wider usage of the data.

ANNEX H: APPLYING THE RECOMMENDATIONS TO THE PUBLIC HEALTHCARE SECTOR

1 Health data within the public healthcare sector should be well-protected, given its sensitive nature.

2 The Committee notes that MOH is committed to improve the protection of health data, and plans to comply with all the PSDSRC recommendations for its public healthcare data and systems. These recommendations will be implemented on top of the existing and planned safeguards that MOH is currently working on, as part of MOH's "defence-in-depth" approach.

3 The Committee recommends that the proposed measures be adopted fully for data used in healthcare policy, research and analytics, and administrative functions. For patient care systems, the measures should be contextualised and implemented in a manner that upholds patient safety and enables better delivery of clinical care. In particular, healthcare professionals need access to accurate and relevant information about a patient in order to identify the right patient, make the right diagnosis and deliver the appropriate treatment. Access to patient data must also be timely, particularly during emergencies.

4 In view of these considerations, not all of the Committee's recommendations will be appropriate and relevant for adoption, given the impact on patient safety and care. For example, hashing patients' identifiers and masking patients' medical records could hinder the healthcare professionals' ability to identify the right patient and make a sound diagnosis or treatment decision.

5 In place of technical or process measures where MOH has assessed that its implementation may adversely impact patient safety and care, MOH will adopt other safeguards to ensure that health data is adequately protected.

6 The Committee notes that the public healthcare system, as with other healthcare systems in most countries, uses specially developed Commercial-Off-The-Shelf (COTS) systems by vendors. The data security in these systems corresponds to the best of class currently available for healthcare systems globally. MOH is working with system vendors to further upgrade their data security and cybersecurity standards to meet new and emerging threats, and will adopt these best of class practices as they become available.

7 The Committee notes that MOH is issuing a HealthTech Instruction Manual which will guide public healthcare institutions on common policies and standards on data governance and security.

ANNEX I: HOW THE RECOMMENDATIONS WOULD ADDRESS A RANGE OF THREAT SCENARIOS

1 The Committee’s recommendations will address a range of threat scenarios and archetypes, such as: (a) Malicious attacker; (b) Negligent insider; (c) Careless employee; and (d) Third Party vendor mishandling Government data. The Committee analysed past data incidents to assess whether the Committee’s recommendations would reduce the possibility or minimise the impact of similar incidents in the future.

2 Each incident typically consists of multiple points of failure which lead to the eventual data incident. While no single measure could decisively prevent or completely eliminate the impact of an incident, the proposed measures would work collectively to more effectively protect data. The following paragraphs summarise how the Committees’ recommendations could more effectively prevent or mitigate the impact of similar data incidents.

Archetype: Malicious Attacker

3 A “malicious attacker” is an actor outside of the organisation that intentionally attempts to compromise the organisation’s data for unauthorised purposes. Malicious attackers range from casual hackers and organised criminals to sophisticated state actors, who may have varied motivations for compromising Government data – from curiosity to gathering intelligence about sensitive entities.

4 In 2018, Singapore suffered its largest cyber-attack at the hands of a malicious attacker. In the SingHealth Cyber Attack, a sophisticated malicious attacker exfiltrated the personal data of 1.5 million patients and specifically targeted the data of key persons.

Example: <i>SingHealth Cyber Attack, 2018</i>		
Stages	What happened	How the Recommendations would address the point of failure
①	A skilled attacker gained entry to the IT network after overcoming a series of security measures. Once inside the network, the attacker compromised privileged accounts to connect to the database.	The proposed technical measure that monitors authorised access and privileged access would have more effectively identified and flagged out the unauthorised use of the privileged accounts.
②	The IT security staff spotted signs of potential intrusions in the IT network but did not recognise that they were indicators of a sophisticated attack.	The proposed increase in training focus for IT security staff would better equip them with tools and expertise to be able to handle a wider range of data security threats and detect signs of a sophisticated attacker.

3	The delayed reporting of the suspicious activity by IT security staff gave the attacker more space and time in the attack.	The proposed Enhanced Data Incident Management Framework would have made clear to the IT security staff that they should promptly report suspected incidents to the relevant parties.
---	----------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Archetype: Negligent Insider

5 A “negligent insider” is an actor within the Singapore Government that has authorised access to the data but did not take reasonable care of the data. An example of a “negligent insider” compromising data is the HIV Registry Leak, where an authorised medical officer is believed to have downloaded the HIV registry data into a thumbdrive and failed to retain possession of it.¹⁰ An unauthorised external party subsequently copied out the HIV registry data and leaked the data onto the Internet.

Example: <i>HIV Registry Leak</i>		
Stages	What happened	How the Recommendations would address the point of failure
1	Sometime in 2012 or 2013, a medical officer, who was an authorised user, is believed to have copied out the HIV registry data into a thumbdrive.	<p>The proposed process safeguard of accessing sensitive files only on secured platforms would have prevented download of data by the medical officer.</p> <p>In addition, the proposed technical safeguard of enhanced logging and active monitoring of data access would have detected anomalous activity such as attempts to copy data out from the platform.</p>
2	The HIV data file is believed to have been later copied by an unauthorised party.	<p>The proposed technical measure of Data Loss Protection Tools would have stopped unauthorised data exfiltration via USB storage device or email.</p> <p>The proposed technical safeguard of limiting and monitoring authorised and privileged access would have restricted the medical officer’s access to the HIV data file to the duration necessary for his work. This would have immediately and automatically terminated the medical officer’s access once he left his position.</p>

¹⁰ The medical officer’s charge in respect of this matter is still pending before the Courts.

3	Files containing the HIV registry data were later leaked onto the Internet by the unauthorised party in 2019.	<p>The proposed technical measure of Digital Watermarking would have identified the source of the leak of the HIV registry data file.</p> <p>The proposed technical measure of tokenisation is suitable for this case as the HIV registry data was used for analytics. The tokenised data would have prevented identification of the individuals even if the data was released.</p>
---	---------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Archetype: Careless Employee

6 A “careless employee” is an employee of the Singapore Government who unintentionally compromises Government data. These are commonly known as “fat finger” incidents, where a public officer inadvertently sends sensitive data to unauthorised recipients.

Example: <i>Data Incident in a Primary School, 2015</i>		
Stages	What Happened	How the Recommendations would address the point of failure
1	An Excel spreadsheet containing the names and birth certificate numbers of all 1,900 pupils in the school and the names, phone numbers and e-mail addresses of their parents was mistakenly sent to about 1,200 parents as part of an update about a school event.	The technical measure of Email Data Protection tool will warn officers that they are sending sensitive data to external parties and would require them to affirm the need to send the data.

Archetype: Third Party Vendor mishandling Government data

7 Public agencies work extensively with third party vendors to deliver services to citizens, carry out operational functions, and provide consultation services for policy analysis and planning. As a result, third party vendors may handle large volumes of Government data and may compromise data should they not safeguard the data well. A recent example of this is the HSA Blood Donor Database Exposure, where the vendor of HSA placed the database on an unsecured server that was accessible from the Internet.

Example: <i>HSA Blood Donor Database Exposure, 2019</i>		
Stages	What happened	How the Recommendations would address the point of failure
①	A vendor was contracted to repair the HSA blood donor database, which had become corrupted. The vendor copied the entire database from HSA.	The proposed process measure of having an Isolated Environment for high-risk scenarios would have required the vendor to access the database in a physically or virtually isolated environment.
②	The vendor placed the database on an unsecured server that was accessible from the Internet to perform the repair.	The proposed Third Party Management Framework for monitoring and auditing the vendor's data security performance would have identified the vendor's unsafe practices.
③	The database was discovered by an IT security expert who reported the incident to PDPC. PDPC informed HSA and access to the database was cut.	The proposed Enhanced Data Incident Management Framework would have provided the security expert with a single reporting point for incident management and response, reducing the time taken to cut the database access and respond to the incident.

ANNEX J: PROPOSED IMPLEMENTATION PLAN

1 The Committee recommends that the Government execute its recommendations as soon as practicable to improve its data security regime. This requires all public agencies to consider their different operating contexts and stakeholders, identify the areas which pose the greatest risk and prioritise measures to execute accordingly. Public agencies also need to take a holistic approach in executing the recommendations. For instance, public agencies should carry out capability-building measures in tandem with technical measures. This is so that public officers *know* how to use data securely when they perform their daily work, and have the *right tools* to do so. Measures should also be implemented in a *user-centric* manner, such that it is intuitive for public officers to follow the right processes and use the appropriate tools to secure data. This may involve process and job redesign.

Measures that have been deployed

2 The Committee notes that as of the release of this report, the Government has already implemented baseline technical measures to strengthen data security standards across the public sector. These measures will result in: (a) data integrity being verified to detect malicious modifications; (b) sensitive data in emails being automatically detected and flagged out; and (c) enhanced encryption for data in files.

Tap on central solutions and build central resources

3 Where possible, the Committee recommends that agencies tap on central technical solutions/systems and that central resources be built (e.g. best practices) to support the implementation of measures. Agencies should actively tap on the Government Data Architecture (GDA) and collect datasets only where necessary; and access sensitive files on platforms where access and usage are centrally logged and monitored. Agencies should also use other central technical platforms and distribution channels such as the Singapore Government – Document Collaboration Service to distribute files. These central technical solutions/platforms will improve the cost effectiveness and consistency of implementation of measures across the public service, while minimising the surface area for attack. Central resources for capability building will also enable learnings to be promulgated across agencies. These central solutions will be particularly helpful to smaller agencies that may not have the right resources to implement such measures on their own.

Implementation based on Risks and Context

4 The safeguards should be implemented based on the data security risks and the unique operating context of each agency. Agencies will therefore need to study the risks of their systems and contextualise the implementation of the safeguards to meet their data security and operational needs. Agencies should also differentiate the implementation of the safeguards in new and existing systems:

- a. All new projects initiated from Oct 2019 onwards should incorporate the technical safeguards from the onset;
- b. Existing systems may require significant re-architecting before the safeguards can be implemented. It may therefore take more time for the measures to be incorporated in these systems; in the meantime, agencies

should put in place other process and people measures to ensure that data is kept secure.

Immediate Implementation Timeline

5 The Committee recommends implementing the measures as soon as practicable. Measures related to processes, people and organisational structures can be implemented earlier, while measures which require the development of new technical solutions will take time to procure and develop.

6 The Committee recommends the following timeline to implement its recommendations:

Key Recommendation 1		31 Oct 2019	30 Apr 2020	31 Oct 2020	2021 and beyond
1.1	Reduce the surface area of attack by minimising data collection, data retention, data access and data downloads	[Timeline bar from 31 Oct 2019 to 2021 and beyond]			
1.2	Enhance the logging and monitoring of data transactions to detect high-risk or suspicious activity	[Timeline bar from 31 Oct 2019 to 2021 and beyond]			
1.3	Protect the data directly when it is stored and distributed to render the data unusable even if extracted	[Timeline bar from 31 Oct 2019 to 2021 and beyond]			
1.4	Keep abreast of advanced technical measures and deploy them when they are mature	[Timeline bar from 31 Oct 2019 to 2021 and beyond]			
1.5	Enhance the data security audit framework to detect gaps in practices and policies before they manifest into incidents	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
1.6	Enhance the third party management framework to ensure that third parties handle Government data with the appropriate protection	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
Key Recommendation 2		31 Oct 2019	30 Apr 2020	31 Oct 2020	2021 and beyond
2.1	Establish a central contact point in the Government Data Office for the public to report Government data incidents	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
2.2	Designate the Government Data Office to monitor and analyse data incidents that pose significant harm to individuals	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
2.3	Designate the Government IT Incident Management Committee to respond to incidents with Severe impact	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
2.4	Institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
2.5	Establish a standard process for post-incident inquiry for all data incidents.	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
2.6	Distil and share learning points with all agencies to improve their data protection policies/measures and response to incidents	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			

Key Recommendation 3		31 Oct 2019	30 Apr 2020	31 Oct 2020	2021 and beyond
3.1	Clarify and specify the roles and responsibilities of groups of public officers involved in the management of data security	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
3.2	Equip these groups with the requisite competencies and capabilities to perform their roles effectively	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			[Timeline bar from 2021 and beyond]
3.3	Inculcate a culture of excellence around sharing and using data securely	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			[Timeline bar from 2021 and beyond]
Key Recommendation 4		31 Oct 2019	30 Apr 2020	31 Oct 2020	2021 and beyond
4.1	Institute organisational Key Performance Indicators (KPIs) for data security	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
4.2	Mandate that the top leadership be accountable for putting in place a strong organisational data security regime.	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
4.3	Make the impact and consequences of data security breaches salient to public officers	[Timeline bar from 31 Oct 2019 to 30 Apr 2020]			
4.4	Ensure accountability of third parties handling Government data by amending the PDPA	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			
4.5	Publish the Government’s policies and standards on personal data protection	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			
4.6	Publish an annual update on the Government’s personal data protection efforts	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			
Key Recommendation 5		31 Oct 2019	30 Apr 2020	31 Oct 2020	2021 and beyond
5.1	Appoint the Digital Government Executive Committee to oversee public sector data security	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			
5.2	Set up a Government Data Security Unit to drive data security efforts across the Government	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			
5.3	Deepen the Government’s expertise in data privacy protection technologies through GovTech’s Capability Centres.	[Timeline bar from 31 Oct 2019 to 31 Oct 2020]			

Implementation of all measures by 31 Dec 2023

7 The Committee recommends that by the end of 2021, the relevant measures will be implemented in 80% of Government systems. The remaining 20% of Government systems require significant re-architecting before the proposed technical measures can be implemented. The Committee recommends that the proposed measures be implemented for these systems by end 2023. In the interim, agencies

must put in place the right process and people measures to manage the attendant data security risks.

Data Security is a continuous journey

8 The Committee recognises that data security is a continuous journey and that new risks will continue to emerge as technology advances. While the Committee's proposed technical, process and people safeguards will strengthen the foundation of the public sector data security regime, it is equally important for the Government to continually enhance its data security posture to take changes in the data security landscape into account. The set-up of the Government Data Security Unit (Recommendation 5.2) and the increased investment in data protection and privacy preservation capabilities through GovTech's Capability Centres (Recommendation 5.3) will enable the Government to keep up-to-date with emerging data security risks and the appropriate technological and process measures to manage these risks.

ANNEX K: SUMMARY OF COMMITTEE'S RECOMMENDATIONS

PUBLIC SECTOR DATA SECURITY REVIEW

Data is a valuable asset. By using it securely, the Government can serve citizens better. The Public Sector Data Security Review Committee was convened to review how the Government secures and protects citizen's data. The Committee has made five key recommendations:



1 Enhance Data Protection and Prevent Data Compromise

- Reduce surface area of attack by minimising data collection, retention, access and downloads
- Enhance logging and monitoring to detect high-risk or suspicious activity
- Protect data directly when stored and distributed to render it unusable even if extracted
- Deploy advanced technical measures
- Enhance data security audit framework
- Enhance third party management framework

2 Enhance Detection and Response to Data Incidents

- **Detect** – Establish central contact point for public to report data incidents
- **Analyse** – Government Data Office to monitor and analyse data incidents
- **Respond** – Central body to respond to large scale incidents
- **Remediate** – Notify individuals significantly impacted
- **Post-Incident Follow-up** – a. Establish standard process for post-incident inquiry
b. Distil and share learning points with all agencies



3 Raise Competencies, Instil Culture of Excellence

- Specify roles and responsibilities of public officers
- Equip groups with competencies to perform role effectively
- Inculcate a culture of excellence in sharing and using data securely

4 Accountability for Data Protection at Every Level

- Institute organisational KPIs for data security
- Mandate top leadership to be accountable for organisational data security
- Make the consequences of data breaches salient to public officers
- Ensure accountability for third parties handling Government data
- Publish the Government's policies and standards on personal data protection
- Publish annual updates on Government's efforts in safeguarding personal data



5 Ensure Sustainability and Resilience

- Appoint high-level Whole-of-Government body to oversee public sector data security
- Set up the Government Data Security Unit to drive public sector data security
- Deepen the Government's expertise in data privacy protection technologies

ANNEX L: LIST OF CONTRIBUTORS

Public Sector Data Security Review Committee (PSDSRC) Members

Mr Teo Chee Hean (Chairman)	Senior Minister; Coordinating Minister for National Security; Minister-in-Charge of Public Sector Data Governance
Dr Vivian Balakrishnan	Minister for Foreign Affairs; Minister-in-Charge of Smart Nation
Mr S Iswaran	Minister for Communication and Information; Minister-in-charge of Cybersecurity
Mr Chan Chun Sing	Minister for Trade and Industry; Minister-in-Charge of the Public Service
Dr Janil Puthucheary	Senior Minister of State, Ministry of Transport and Ministry of Communications and Information, and Minister-in-Charge of Government Technology Agency
Sir Andrew Witty	Chief Executive, Optum
Professor Anthony Finkelstein	Chief Scientific Adviser for National Security, UK Government
Mr David Gledhill	Senior Advisor and Former Chief Information Officer, DBS
Mr Ho Wah Lee	Independent Board Director, NTUC Fairprice Cooperative Ltd
Mr Lee Fook Sun	Chairman, Ensign Infosecurity

Expert Group

Mr Arthur Wong	Singtel Chief Executive of Global Cybersecurity
Mr Huey Tan	President, Asia Data Protection Officers (AsiaDPO)/Senior Privacy Counsel, Asia-Pacific, Apple
Mr Keng Seng Wei	Managing Director, Technology Services & Information Security Services, DBS
Dr Lee Shiang Long	President, Land Systems, ST Engineering
Dr Robert JT Morris	Chief Technology Strategist MOHT, and Professor, Yong Loo Lin School of Medicine, NUS
Professor Simon Chesterman	Dean, NUS Faculty of Law
Ms Wu Choy Peng	Chief Technology Officer, GIC

Taskforce

Mr Ng Chee Khern (Chairman)	Permanent Secretary, Smart Nation and Digital Government
Mr Kok Ping Soon	Chief Executive, Government Technology Agency, Chairman of Workgroup (Practices)
Mr Tan Kok Yam	Deputy Secretary, Smart Nation and Digital Government, Chairman of Workgroup (Policies and Measures)

Mr Chan Cheow Hoe	Government Chief Digital Technology Officer and Deputy Chief Executive, Government Technology Agency, Co-Chairman of Workgroup (Policies and Measures)
Mr Janadas Devan	Chief of Government Communications, Chairman of Workgroup (Communications and Engagement)
Mr David Koh	Chief Executive, Cyber Security Agency
Ms Ngiam Siew Ying	Deputy Secretary (Policy), Ministry of Health
Mr Tan Kiat How	Chief Executive, Infocomm Media Development Authority
Ms Tan Li San	Deputy Secretary, Ministry of Communications and Information
Ms Teoh Zsin Woon	Deputy Secretary (Transformation), Public Service Division
Ms Wong Wee Kim	Chief Statistician

Workgroup (Policies and Measures)

Mr Tan Kok Yam (Chairman)	Deputy Secretary, Smart Nation and Digital Government
Mr Chan Cheow Hoe (Co-Chairman)	Government Chief Digital Technology Officer and Deputy Chief Executive, Government Technology Agency, Smart Nation and Digital Government Office
Mr Chai Chin Loon	Senior Director, Government Technology Agency
Ms Gwenda Fong	Senior Director, Strategy and Planning, Cyber Security Agency
Mr Jason See	Director, Chief Information Officer, Ministry of Defence
Ms Lim Bee Kwan	Assistant Chief Executive, Government Technology Agency
Mr Ng Sy Horng	Assistant Commissioner, Inland Revenue Authority of Singapore
Ms Ngiam Siew Ying	Deputy Secretary (Policy), Ministry of Health
Mr Phua Hooi Boon	Senior Director, Technology and Logistics Policy Division, Ministry of Home Affairs
Ms Teoh Zsin Woon	Deputy Secretary (Transformation), Public Service Division
Mr Terence Ho	Division Director, Manpower Planning and Policy Division, Ministry of Manpower
Ms Wong Wee Kim	Chief Statistician
Mr Yeong Zee Kin	Assistant Chief Executive, Infocomm Media Development Authority

Workgroup (Practices)

Mr Kok Ping Soon (Chairman)	Chief Executive, Government Technology Agency
Mr Adrian Cheong	Group Director, Accountant-General's Department
Mr Chong Quey Lim	Chief Technology Officer, Central Provident Fund Board
Ms Jeanette Khong	Information Service Manager, Government Technology Agency

Ms Lim Bee Kwan	Assistant Chief Executive, Government Technology Agency
Mr Lim Hwee Kwang	Director, Defence Science & Technology Agency
Mr Lim Thian Chin	Director, Cyber Security Agency
Mr Ng Sy Horng	Assistant Commissioner, Inland Revenue Authority of Singapore
Mr Ong Chin Ann	Chief Information Officer, Public Service Division
Mr Ong Leong Seng	Group Director, Integrated Health Information Systems
Mr Quah Choo Seng	Group Director, Housing Development Board
Mr Tan Eng Pheng	Assistant Chief Executive, Government Technology Agency
Ms Tan Sor Hoon	Chief Information Office, Immigration and Checkpoints Authority
Mr Yeong Zee Kin	Deputy Commissioner, Personal Data Protection Commission; Assistance Chief Executive, Infocomm Media Development Authority

Workgroup (Communications and Engagement)

Mr Janadas Devan (Chairman)	Chief of Government Communications
Ms Alamelu Subramaniam	Senior Director, Media Division, MCI
Mr Atticus Foo	Deputy Director, Messaging and Engagement, MCI
Ms Deanna Mohd Isnin	Assistant Director, Messaging and Engagement, MCI
Mr Jimmy Toh	Deputy Chief of Government Communications (Ops)
Ms Joyce Yong	Senior Manager, Messaging and Engagement, MCI
Ms Nasrath Hassan	Senior Assistant Director, Adoption and Engagement Directorate, SNDGO
Ms Shakera Stationwala	Director, Messaging and Engagement, MCI

Secretariat

Ms Quek Su Lynn (Head, Secretariat)

Ms Alice Yeo	Mr Joseph Lee
Mr Alvin Yeo	Ms Joyce Tan
Mr Bryan Loh	Mr Lim Yin Pieu
Mr Brian Yeoh	Ms Loh Shin Yee
Mr Chau Chee Chiang	Ms Mah Yu Ling
Ms Cheng Jing Yi	Mr Martin Chew
Mr Chin Hui Han	Ms Nasrath Hassan
Mr Desmond Tan	Mr Paul Ng
Mr Francis Zhang	Ms Rebecca Lim
Ms Geraldine Pang	Ms Ruth Poh
Ms Goh Shi Min	Mr Stephen Sim
Ms Jessica Ang	Mr Teo Yi Heng
Mr Goh Yu Chong	Mr Zachary Ang