

# **PUBLIC SECTOR DATA SECURITY REVIEW COMMITTEE REPORT**

---

**November 2019**



# EXCHANGE OF LETTERS WITH THE PRIME MINISTER

26 November 2019

Prime Minister

In March 2019, you convened the Public Sector Data Security Review Committee (PSDSRC) to conduct a comprehensive review of data security practices across the entire public service.

2 The Committee has completed its work and now submits its report for your consideration. The report contains five key recommendations for the public sector, which when implemented would: (a) Effectively protect against data security threats and minimise the occurrence of data incidents; (b) Detect and respond to data incidents in a swift and decisive manner, and learn from each incident; (c) Build data security competencies and inculcate a culture of excellence around sharing and using data securely; (d) Raise the accountability and transparency of the public sector data security regime; and (e) Put in place the organisational structures to sustain a high level of security, and to be adaptable to new challenges.

3 In arriving at these recommendations, the Committee examined the current state of data security practices in public agencies. We also studied the approaches taken by companies and other governments, and compared public sector data security standards with those stipulated for the private sector under the Personal Data Protection Act. Finally, we checked whether our recommendations would have prevented, or mitigated the impact of, past data incidents in the public and public healthcare sector.

4 We are satisfied that our recommendations are comprehensive and robust; and that they provide the basis for the Government to continue to use data securely and effectively to make policy decisions, and to deliver a high quality of service to citizens. We hope that these recommendations will also give the public confidence that their data entrusted to public agencies is well protected.

5 Our report also contains an action plan to implement the recommendations as soon as practicable. We note that the Government has already implemented three baseline technical measures identified earlier by the Committee to improve data security standards.

6 The launch of this review was partly triggered by several data breaches that occurred in our healthcare sector. The Ministry of Health (MOH) plans to fully comply with all the recommendations for its public healthcare systems and data used for healthcare policy, research and analytics, and administrative functions. MOH will further study how the measures can be contextualised and implemented in patient care systems, in a manner that upholds patient safety and enables better delivery of clinical care, while taking into account the unique operational requirements of the healthcare sector. MOH will also study and consult licensees and entities handling health data on further ways to safeguard the collection, storage, use and sharing of health information, including through legislation and licensing requirements.

7 Finally, we would like to acknowledge the contributions of the members of the Expert Group. Their involvement in the process has enabled us to draw from a wider pool of knowledge and experience from different industry sectors.



---

Mr Teo Chee Hean



---

Dr Vivian Balakrishnan



---

Mr S Iswaran



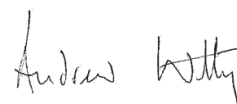
---

Mr Chan Chun Sing



---

Dr Janil Puthucheary



---

Sir Andrew Witty



---

Professor Anthony Finkelstein



---

Mr David Gledhill



---

Mr Ho Wah Lee



---

Mr Lee Fook Sun





*Prime Minister  
Singapore*

27 November 2019

Senior Minister Teo Chee Hean  
Chairman, Public Sector Data Security Review Committee

Thank you for your letter dated 26 November 2019, submitting the recommendations of the Public Sector Data Security Review Committee (PSDSRC).

Data is the lifeblood of the digital economy and a digital government. We need to use and share data as fully as possible to provide better public services. In doing so, we must also protect the security of the data and preserve the privacy of individuals, and yet not stifle digital innovation. This is especially so in healthcare, but it is true of every other field of government too.

As the custodian of a vast amount of data, the Government takes this responsibility very seriously. We must do our utmost to minimise the risk of data breaches. At the same time, when such breaches do occur, as unfortunately they occasionally will, it is essential that we detect them quickly, and respond effectively to limit the breach and minimise the harm done.

This is why I convened the PSDSRC in March 2019. I am pleased that the PSDSRC has put together a comprehensive report. You have consulted widely, studied international best practices, and recommended technical, procedural and organisational changes to improve our ability to manage data confidently and securely, and enable the Government to deliver better services and policies for Singaporeans.

The Government accepts the Committee's recommendations in full. Your proposals are practical, and we will implement them expeditiously and thoughtfully. At the same time, given how quickly digital technology is changing, we will continually review our implementation of data security measures, so that the specific measures taken are always up to date and fit for purpose.

On behalf of the Government, I thank you and your Committee members, the Expert Group, the Taskforce and the working groups for their contributions. I am sure we can continue to count on their advice and support in the coming years, as we work towards our vision of building a Smart Nation.

A handwritten signature in blue ink, reading "Lee Hsien Loong".

LEE HSIEN LOONG

# OVERVIEW

1 Data is a valuable asset that can bring about tremendous opportunities for individuals and societies. It has the potential to improve lives and strengthen communities. While the Government uses a wide range of data, including personal data, to serve citizens, it must do so in a manner that ensures the information is secured. Failure to safeguard sensitive data can lead to serious harm to individuals and/or national security.

2 Several data incidents uncovered in 2018 and 2019 highlighted the need to review the Government's information security policies and practices, and strengthen the data security regime against current and future threats. This is especially important as the Government's ICT systems are increasingly integrated and data is used and shared more widely to deliver better services to citizens. It was in this context that the Prime Minister convened the Public Sector Data Security Review Committee (from here on referred to as "the Committee").

## Terms of Reference of the Committee

The Committee's Terms of Reference are to:

- Review how the Government is securing and protecting citizens' data from end-to-end, including the role of vendors and other authorised non-Government Entities;
- Recommend technical measures, processes and capabilities to improve the Government's protection of citizens' data, and response to incidents; and
- Develop an action plan of immediate steps and longer-term measures to implement the recommendations.

## The Committee's Approach

In formulating its recommendations, the Committee:

- Conducted a comprehensive review and inspection of 336 systems across 94 public agencies to identify risk areas and common causes of data breaches.
- Studied global and industry best practices, including the practices of the Governments of Canada and the United Kingdom, and companies in the finance and security sectors.
- Reviewed the Government's data security related legislation and guidelines i.e. Instruction Manual 8 (IM8) and Public Sector (Governance) Act (PSGA) against the requirements for private sector organisations in the Personal Data Protection Act (PDPA).
- Evaluated whether the proposed recommendations would have prevented, or significantly mitigated the impact of, the data incidents uncovered in 2018 and 2019.

3 The Committee's work built on the Government's ongoing efforts to strengthen the secure usage and sharing of data, through continually improving policies, legislation, measures and organisational structures.

4 Since 2001, the Government's data security standards have been set out in the IM8. Subsequently, the Personal Data Protection Act or PDPA was enacted in 2012 to govern data protection in the private sector, taking reference from the IM8 standards<sup>1</sup>.

5 In 2018, additional data security provisions were included in the PSGA to further deter the mismanagement of Government data and strengthen the Government's data security regime. The Committee has reviewed the IM8 and the PSGA and are satisfied that the data protection requirements imposed on the Government are no less stringent than the PDPA's. In addition, the IM8 contains specific standards and guidelines to ensure that these data protection requirements are well met within the public sector. While the IM8 and the PDPA currently use similar language to describe the data protection requirements, the Committee recommends further alignment of the language in the IM8 and the PDPA for greater consistency and clarity.

6 Through its inspection of the key systems and data management practices<sup>2</sup> of all 94 public agencies and its study of global and industry best practices, the Committee found areas for improvement in the Government's policies and practices. Agencies, particularly smaller agencies, can be better supported in implementing the policies as intended. Officers' roles and responsibilities in data security can be more clearly articulated. There are also best practices in technical, process and organisational measures that the Government can adapt to bolster the data security regime, and ensure consistently high levels of data security across the public sector. For example, there are technical tools that should be applied more widely to ensure consistently high compliance with data security measures across the public sector. The Government's high standards of data protection will need to extend to vendors and other non-Government Entities that handle public sector data when they provide services to the public sector. Additionally, the management of data-related incidents can be further tightened, including standardising processes for the public to report incidents and to be notified of incidents and formalising review processes to learn from incidents. These identified gaps and risks have informed the Committee's recommendations.

<sup>1</sup> Refer to **Annex A** for existing Government efforts to improve secure data usage.

<sup>2</sup> Refer to **Annex B** for an overview of the inspection and stock-take of data management practices.

# COMMITTEE'S RECOMMENDATIONS

7 The Committee's recommendations will address existing gaps and build a data security regime that is resilient as technology advances, systems become more integrated, and risks become increasingly multi-faceted. The recommendations will provide a strong foundation for the Government to share and use data to serve citizens effectively. The recommendations will be regularly reviewed to ensure that they remain relevant and effective.

## ***Desired Outcomes***

8 The Committee's recommendations, when implemented, will ensure that the Government effectively (a) protects data and prevents data compromises, (b) detects and responds to data incidents, (c) with competent public officers embodying a culture of excellence, (d) accountability for data protection at every level, and (e) in a sustainable and resilient manner.

## ***Key Recommendations***

9 The Committee has made **five key recommendations** to achieve the desired outcomes. These recommendations cover Government and non-Government Entities that handle public sector data to deliver public services, perform operational processes, or provide consultation services for policy planning.

| <b>Desired Outcomes</b>   | <b>Key Recommendations</b>   |
|---|--|
| <b>Protects data and prevents</b> data compromises                        | 1. Enhance technology and processes to effectively protect data against security threats and prevent data compromises.                                   |
| <b>Detects and responds to</b> data incidents                             | 2. Strengthen processes to detect and respond to data incidents swiftly and effectively.   |
| <b>Competent</b> public officers embodying a <b>culture of excellence</b> | 3. Improve culture of excellence around sharing and using data securely, and raise public officers' competencies in safeguarding data                    |
| <b>Accountability</b> for data protection at every level                  | 4. Enhance frameworks and processes to improve the accountability and transparency of the public sector data security regime                             |
| <b>Sustainable and resilient manner</b>                                   | 5. Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime that can meet future needs. |





## Key Recommendation 1: Enhance technology and processes to effectively protect data against security threats and prevent data compromises<sup>3</sup>.

10 The Committee has proposed 13 technical (prefixed with 'T') and 10 process safeguards (prefixed with 'P'). These will be incorporated into ICT and data systems in different combinations depending on the data security risks that the system is expected to face. They will minimise the risk of data compromises by achieving the following:

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



### Collect and retain data only when necessary

**P1:** Collect datasets only where necessary

**P2:** Limit retention period of data



### Minimise the proliferation of data to endpoint devices

**P3:** Isolated Secured Environments for third parties and privileged users

**P4:** Access data by queries instead of data dumps

**P5:** Access sensitive files on secured platforms



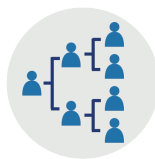
### Access and use data for the task at hand

**T1:** Volume limited and time limited data access

**T2:** Automatic Identity and Access Management Tools

**P6:** Limit and monitor authorised and privileged access

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



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

**P7:** Maintain data lineage

**T3:** Digital watermarking of files



### Detect suspicious activity and alert the user or stop the unauthorised activity automatically

**T4:** Enhanced logging and active monitoring of data access

**T5:** Email data protection tool

**T6:** Data loss protection tool

<sup>3</sup> Refer to **Annex C** for more details of Key Recommendation 1.

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



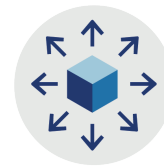
**Render data unusable even if exfiltrated from storage**

- T7:** Hashing with salt
- T8:** Tokenisation
- T9:** Field-level encryption
- P8:** Managing keys to these safeguards



**Partially hide the full data**

- T10:** Obfuscation/ masking/ removal of entity attributes
- T11:** Dataset partitioning



**Protect the data during distribution**

- T12:** Password protecting and encrypting data files
- P9:** Securely distribute password out-of-band
- T13:** Data file integrity verification
- P10:** Distribute files through appropriate secure channels

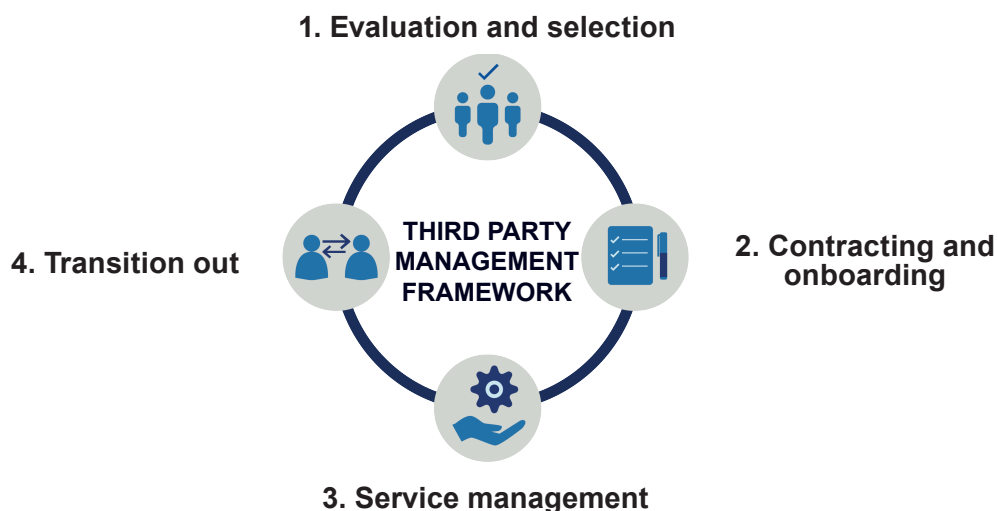
11 Beyond the 13 technical and 10 process measures, the Committee makes the following recommendations to better protect data against data security threats:

**Recommendation 1.4:** Develop and maintain expertise in advanced technical measures<sup>4</sup>.

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

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

12 The third party management framework of Recommendation 1.6 is structured around the four stages of the third party management lifecycle:



<sup>4</sup> The Committee has identified six advanced technical measures, which are not sufficiently mature or readily integrable today for widespread implementation: (i) Homomorphic Encryption; (ii) Multi-party authorisation; (iii) Differential Privacy; (iv) Dynamic Data Obfuscation and Masking; (v) Digital Signing of Data File; and (vi) Secured File Format.



## Key Recommendation 2: Strengthen processes to detect and respond to data incidents swiftly and effectively<sup>5</sup>.

13 Even with additional measures to protect data and prevent data compromises, it is impossible to eliminate data incidents entirely. It is therefore vital that the Government remains vigilant and prepared for data compromises to effectively contain any damage, take remedial action and learn from each incident. Key Recommendation 2 includes measures that will strengthen the Government's existing processes to detect threats, and to respond to a data incident swiftly and effectively. This will enable the Government to contain the damage, eradicate the threat and restore systems/operations should a data incident occur.

14 The Committee's recommendations for managing data incidents are structured around the five stages of "Detect", "Analyse", "Respond", "Remediate" and "Post-Incident Follow-up":

### 1. Detect



**Recommendation 2.1:** Establish a central contact point for the public to report Government data incidents. This complements the current processes for agencies to report Government data incidents to the Smart Nation and Digital Government Group.

### 2. Analyse



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

### 3. Respond



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

### 4. Remediate



**Recommendation 2.4:** Institute a framework for all public agencies to promptly notify individuals affected by data incidents with significant impact to the individual. This notification framework and the proposed PDPA amendments in 2020 for a mandatory data breach notification regime will be the same.

### 5. Post-Incident Follow-up



**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.

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

<sup>5</sup> Refer to **Annex D** for more details of Key Recommendation 2.



### Key Recommendation 3: Build a culture of excellence in sharing and using data securely and raise public officer's competencies in safeguarding data<sup>6</sup>.

15 Public officers must be alert to data security risks when handling citizens' data. The recommended safeguards will be effective only if they are well executed by public officers. It is important that officers understand their roles and be equipped to fulfil their responsibilities. This goes beyond compliance with rules and tasks. Such compliance only establishes a baseline level for data security and largely addresses data security threats of the past. For the public sector data security regime to be resilient to emerging threats, officers must be sensitive to new risks and proactively take steps to address these risks and safeguard data.

#### GROUPS OF PUBLIC OFFICERS

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



##### Top Leadership



##### Key Appointment Holders

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



##### ICT, Cyber and Data Teams



##### All Public Officers

16 For each group, the Committee proposes the following:

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

**Recommendation 3.2:** Equip these groups with the requisite competencies and capabilities to perform their roles effectively. This includes ensuring that all public officers are regularly updated on data security considerations, for example, through an annual training programme and declaration.

**Recommendation 3.3:** Inculcate a culture of excellence around sharing and using data securely, for example, through cultivating an environment conducive to open reporting of data incidents whether major or minor.

<sup>6</sup> Refer to **Annex E** for more details of Key Recommendation 3.



## Key Recommendation 4: Enhance frameworks and processes to improve public visibility of the management of and accountability for public sector data security<sup>7</sup>.

### *Improve Accountability of Organisations, Leaders and Individuals*

17 The Committee recognises that the Government has existing accountability frameworks and legislation to hold leaders and individuals accountable for all issues under their purview, including data incidents. These accountability measures range from counselling to financial penalties to dismissal. Additionally, public officers who have recklessly or maliciously mishandled Government data are liable for a fine of up to \$5,000 and/or up to 2 years' imprisonment under the PSGA.

18 The Committee notes that the Government does not impose financial penalties and sanctions on public agencies as such monies come from the same public purse. The more effective measure is to hold those in positions of responsibility accountable for their organisations' effectiveness in maintaining data security, and to take action against individual officers who have allowed data security to be compromised:

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

**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.

19 At the public officer level, the Committee found that not all public officers have internalised the potential impact of their actions on individuals whose data have been compromised, or how such compromise can affect the Government/agency's ability to perform their functions effectively. Public officers are also not aware of the consequences they could bear because of data lapses. The Committee recommends that the Government:

**Recommendation 4.3:** Make the impact and consequences of data security breaches salient to public officers. This could be through data security training programmes and an annual acknowledgement of such policies.

<sup>7</sup> Refer to **Annex F** for more details of Key Recommendation 4.



## ***Improve Accountability of Third Parties***

20 For third parties handling Government data, the Committee recommends tightening the legislation governing the accountability of non-Government Entities that act on behalf of public agencies, and non-Public Officers who recklessly or maliciously mishandle Government data. This is particularly important as the Government works more closely with third parties to deliver services to the public. Therefore, the Committee recommends the following legislative amendments:

**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.

21 Recommendation 4.4(b) will bring the PDPA in line with the PSGA, and reinforce individuals' responsibility and accountability for the personal data they handle by imposing measures on individuals who recklessly or maliciously mishandle personal data.

## ***Improve Transparency***

22 Although the Government has standards which are comparable to, if not more stringent than, the PDPA, the Committee recommends that the Government improve its communication with the public to address their concerns on the Government's use and protection of their data. This will enable the Government to uphold and maintain public confidence in its management of data. The recommendations are:

**Recommendation 4.5:** Publish the Government's policies and standards relating to personal data protection. This will enable the public to understand the Government's approach to personal data protection and the measures in place to protect data.

**Recommendation 4.6:** Publish an annual update on the Government's efforts in safeguarding personal data to provide the public with visibility over the Government's efforts to continually improve its data protection standards.



## Key Recommendation 5: Introduce and strengthen organisational and governance structures to drive a resilient public sector data security regime<sup>8</sup>.

23 While the Government bolsters its technical, process and people safeguards, the Committee recommends that it institutionalise such efforts to ensure that they are sustained and continue to evolve to address new challenges. Currently, data security functions exist in pockets throughout the Government, and responsibility for such functions is diffused. To ensure that the Government manages data security as a strategic consideration and drives data security across the public sector as a Whole-of-Government (WoG) priority in a sustained manner, the Committee proposes the following:

**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.

**Recommendation 5.2:** Set up the Government Data Security Unit in the Government Data Office to drive data security efforts in the Government.

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

<sup>8</sup> Refer to **Annex G** for more details of Key Recommendation 5.

## Public Healthcare Sector<sup>9</sup>

24 The Committee paid particular attention to the governance and security of health data, given the sensitivity of health data. 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 Committee recommends that the measures be contextualised and implemented in a manner that upholds patient safety and enables better delivery of clinical care.

25 The Committee notes that the Ministry of Health (MOH) plans to fully comply with all the recommendations for its public healthcare systems and data. The Committee further notes that MOH is issuing a HealthTech Instruction Manual to guide Public Healthcare Institutions on implementing data security measures. MOH is also enhancing incident preparedness, and raising data security consciousness. These build on MOH's existing structures and processes to ensure regular review of its data security risks and implement measures as part of its "defence- in-depth" approach.

26 Beyond the public sector, MOH has issued cybersecurity advisories to its healthcare licensees to advise them on measures to safeguard their systems and data. MOH will be working with licensees to develop more specific and customised cybersecurity guidelines in the first half of 2020, and support them in improving their cyber and data security posture. MOH will also study and consult licensees and entities handling health data on further ways to safeguard the collection, storage, use and sharing of health information, including through legislation and licensing requirements. Collectively, these efforts will uplift the data and cyber security readiness of the wider healthcare sector.

<sup>9</sup> Refer to **Annex H** for more details of the application of the recommendations to the public healthcare sector

# ADDRESSING A RANGE OF THREAT SCENARIOS<sup>10</sup>

27 The Committee's recommendations address a range of threat scenarios and archetypes observed in data incidents, 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. While no single measure could decisively stop or completely eliminate the impact of an incident, the proposed measures would work collectively to more effectively protect data.



## Type of Data Incident: Malicious External Attacker

Example: SingHealth Cyber Attack, 2018

### Key issues:

The skilled attacker overcame a series of security measures and compromised privileged accounts to access the database. The IT security staff spotted signs of potential intrusions in the IT network but did not recognise them as indicators of a sophisticated attack. The delayed reporting of the suspicious activity by IT security staff gave the attacker more space and time in the attack.

### How the Committee's recommendations might mitigate similar incidents:

The proposed measure to monitor access of authorised and privileged users would more effectively identify and flag out unauthorised use of privileged accounts. The proposed increase in training focus for IT security staff would better equip them with tools and expertise to handle a wider range of data security threats and detect signs of a sophisticated attacker. The proposed Enhanced Data Incident Management Framework would make clear to the IT security staff that they should promptly report suspected incidents to the relevant parties.



## Type of Data Incident: Negligent Insider

Example: HIV Registry Leak

### Key issues:

Sometime in 2012 or 2013, a medical officer is believed to have downloaded a copy of the HIV registry on his thumbdrive and failed to retain possession of it. An unauthorised external party subsequently leaked the HIV registry data on the Internet in 2019.

### How the Committee's recommendations might mitigate similar incidents:

The proposed technical and process safeguards would detect anomalous activity, prevent the download of data via USB storage or email, and identify the source of the leaked file on the Internet for remediation. In addition, the proposed technical safeguard of tokenisation (which would be applied as the data would be used for analytics) would prevent identification of the individuals, even if the data was released.

<sup>10</sup> Refer to **Annex I** for more details of how the measures will address a range of threat scenarios



### **Type of Data Incident: Careless Employee**

**Example: Data Incident in a Primary School, 2015**

#### **Key issues:**

The officer did not check the email recipients list when sending sensitive data. As a result, the officer mistakenly sent the personal details of all 1,900 pupils in the school to about 1,200 parents as part of an update on a school event.

#### **How the Committee's recommendations might mitigate similar incidents:**

The proposed Email Data Protection tool would warn the public officer that he/she is sending sensitive data to external parties and would require him/her to affirm the sending of the email before doing so.



### **Type of Data Incident: Third Party Vendor Mishandling Government Data**

**Example: HSA Blood Donor Database Exposure, 2019**

#### **Key issues:**

A vendor was contracted by HSA to repair the blood donor database. The vendor placed the database on an unsecured server that was accessible from the Internet. The unauthorised disclosure of data was subsequently discovered by an IT security expert.

#### **How the Committee's recommendations might mitigate similar incidents:**

The proposed Third Party Management Framework would guide the agency in monitoring and auditing the vendor's data security performance, identifying unsafe practices, and ensuring compliance with the data security policies.



# IMPLEMENTATION PLAN<sup>11</sup>

28 The Committee has proposed an implementation approach and action plan to ensure that its recommendations are executed promptly and holistically.

29 The Committee notes that as of the release of this report, the Government has implemented baseline 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.

30 The Committee has proposed further technical and process measures to protect citizens' data and recommends that the Government implement these measures as soon as practicable. Implementation of the measures should be calibrated according to the applicable data security risks so that data is neither over- nor under-protected. 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. The Enhanced Data Security Audit framework and Third Party Management Framework will be implemented by 30 April 2020. All public officers will undergo a baseline data security literacy course by 31 October 2020.

31 These measures will reduce the occurrence of data incidents but cannot prevent all incidents from occurring. The Committee has therefore recommended that processes be improved to enable the Government to promptly respond and take remedial actions should data incidents occur. These recommendations will be implemented by 30 April 2020.

32 The Committee notes that implementing these recommendations would involve concerted and focused action and monitoring by the Digital Government Executive Committee. 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, the Government will need 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 GovTech's Capability Centres to deepen the Government's data privacy protection capabilities (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.

<sup>11</sup> Refer to **Annex J** for more details of the proposed implementation plan.

# CONCLUSION

33 The Committee is confident that the recommendations, when implemented, will significantly improve the Government's data security regime and enhance the public's confidence in the Government's data security regime. The recommendations will secure the data at a level of vigilance that goes significantly beyond the baseline that the private sector needs to fulfil to meet PDPA requirements. This will help to establish a culture of excellence in data security within the Government, and enable agencies, public officers and vendors to use data well to serve the public better.

## LIST OF ANNEXES

- Annex A** Existing Government Efforts on Using Data Securely
- Annex B** Inspection of Agencies' Data Management Practices – Overview of Approach and Findings
- Annex C** Key Recommendation 1 – Technical and Process Measures to Protect Data and Prevent Data Compromises
- Annex D** Key Recommendation 2 – Enhanced Data Incident Management Framework
- Annex E** Key Recommendation 3 – Measures to Raise Public Officers' Competencies and Inculcate a Culture of Excellence in Using Data Securely
- Annex F** Key Recommendation 4 – Measures to Improve Accountability and Transparency
- Annex G** Key Recommendation 5 – Organisational and Governance Structures
- Annex H** Applying the Recommendations to the Public Healthcare Sector
- Annex I** How the Recommendations would Address a Range of Threat Scenarios
- Annex J** Proposed Implementation Plan
- Annex K** Summary of Committee's Recommendations
- Annex L** List of Contributors

