



DIGIPIXEL DATA BREACH MANAGEMENT PLAN

Note 1. : Organisations can reference the Guide to Managing and Notifying Data Breaches for considerations to develop their data breach incident response and data breach management plan.

Note 2.: To contain and recover from a cyber incident effectively, our organization may also incorporate the Cyber Incident Response Checklist in **Annex IV**.

1. Definition of Data Breach

1.1 A data breach, in relation to personal data, refers to any unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data. It also includes the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, or disposal of the personal data is likely to occur.

1.2 **Data** breaches can occur for different reasons. Possible activities (non-exhaustive) that may result in a data breach are as follows:

- - i. Loss of computer notebooks, data storage devices, or physical documents containing personal data
 - ii. Sending personal data to a wrong e-mail address or physical address, or disclosing personal data to unintended recipient(s)
 - iii. Unauthorised access or disclosure of personal data by employees
 - iv. Improper disposal of personal data (e.g., hard disk, storage media or physical documents containing personal data sold or discarded before data is properly deleted)
 - v. Poor cyber hygiene practices such as poor password policies. Such policies may comprise weak or poor passwords, no scheduled password changes, sharing of password for administrative accounts etc.

2. Data Breach Management Team

2.1 The data breach management team composition and responsibilities are shown in the appended table.

Data Breach Management Team		
Who	Position	Responsibilities
Tan Yong Li	Team Leader	- Manage incident reports - File incident report to PDPC if necessary
Dave Gurbani & Isaac Raj	Assistant Team Leader	- Monitor data breach incident - Draft incident reports
Tan Yong Li	Member	- Send notifications to affected individuals if necessary
Tan Yong Li	Member	- Communications with staff on data breach incident
Islam MD Tarccqul & Isaac Raj	Member	- Monitor cyber and IT related data incidents

3. Data Breach Response Plan

The data breach management team will follow the four key steps (i.e. Contain, Assess, Report, Evaluate) and take appropriate actions in the event of a data breach.

3.1 Contain the Breach

3.1.1 Staff will report to BU Heads as soon as a data breach (defined in Section 1.1) is suspected or confirmed.

3.1.2 BU Heads will then inform the DPO regarding the potential data breach. DPO will activate the data breach management team and update senior management on potential data breach.

3.1.3 Data breach management team will conduct an initial assessment to determine the severity of the data breach.

3.1.4 The initial assessment will include the following considerations

- Cause of the data breach and whether the breach is still ongoing;
- Number of affected individuals;
- Type(s) of personal data involved;
- The affected systems, servers, databases, platforms, services etc;

- e. Whether help is required to contain the breach; and
- f. The remediation action(s) that the organisation has taken or needs to take to reduce any harm to affected individuals resulting from the breach.

3.1.5 Upon completion of the initial assessment, the data breach management team shall determine the immediate actions to be taken to contain the data breach as soon as possible. Organisations can consider the following immediate containment actions, where applicable:

- a. Isolate the compromised system from the Internet or network by disconnecting all affected systems;
- b. Re-route or filter network traffic, firewall filtering, closing particular ports or mail servers;
- c. Prevent further unauthorised access to the system. Disable or reset the passwords of compromised user accounts;
- d. Isolate the causes of the data breach in the system, and where applicable, change the access rights to the compromised system;
- e. Stop the identified practices that led to the data breach; or
- f. Establish whether the lost data can be recovered and implement further action to minimise any harm caused (e.g. remotely disabling a lost notebook containing a personal data of individuals, recalling an email that has been accidentally sent or forwarded etc.)

3.1.6 Details of the data breach and post-breach response(s) shall be recorded in the Incident Record Log found in **Appendix I**.

3.2 Assess the Data Breach

3.2.1 Upon the containment of the data breach, the data breach management team shall conduct an in-depth assessment of the data breach, the success of its containment action(s) taken, or the efficacy of any technological protection applied on the personal data involved in the data breach.

3.2.2 The data breach management team must assess if the data breach is a notifiable one within 30 calendar days.

3.2.3 The data breach management team shall consider the following in the assessment of the data breach:

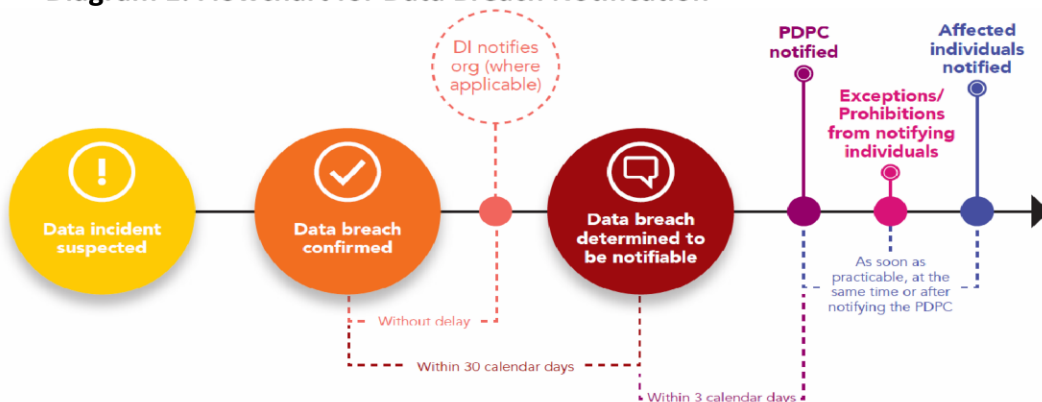
- a. Context of the data breach;
- b. Ease of identifying individuals from the compromised data; and
- c. Circumstances of the data breach.

3.3 Report the Data Breach

3.3.1 The DPO shall notify the PDPC and/or the affected individuals from the time the data breach management team has determined that the data breach is notifiable as shown in Diagram 1.

Note: Where a data breach affects 500 or more individuals, the organisation is required to notify the PDPC, even if the data breach does not involve any prescribed personal data in the Personal Data Protection (Notification of Data Breaches) Regulations 2021.

Diagram 1: Flowchart for Data Breach Notification



3.3.2 The timeframe for a notifiable data breach is as follows:

- The PDPC as soon as practicable, but in any case, no later than three (3) calendar days; and
- Where required, the affected individuals as soon as practicable, at the same time or after notifying the PDPC.

Note: Data breaches which are likely to attract widespread public attention and/or interest, or those which organisations require guidance on notifying the affected individuals, or those which organisations require guidance on notifying the affected individuals, the DPO is strongly encouraged to notify and seek advice from the PDPC first before notifying the affected individuals.

3.3.3 The DPO shall submit the notification to the PDPC at <https://eservice.pdpc.gov.sg/case/db>. For urgent notification of major cases, the DPO shall contact the PDPC at +65 6377 3131 during work hours.

3.3.4 The key information to be provided in the notification to the PDPC and affected individuals in **Appendix II** and **Appendix III** respectively.

3.3.5 The DPO shall notify a sectoral regulator or law enforcement agency of a data breach under other written laws, and shall also notify the PDPC and/or affected individuals (if required) according to the timeframes for data breach notification.

3.4 Evaluate the Response to the Data Breach

3.4.1 The data breach management team shall review and learn from the data breach to improve on their personal data handling practices.

3.4.2 The review may involve the following:

- a. A review including a root cause analysis of the data breach
- b. A prevention plan to prevent similar data breaches in future
- c. Audits to ensure prevention plan is implemented
- d. A review of existing policies, procedures, and changes to reflect the lessons learnt from the review
- e. Changes to employee section and training practices
- f. A review of data Intermediaries involved in the data breach

Note: Organisations may incorporate other relevant areas in its post-breach evaluation in **Appendix V**.

Appendix I	Data Breach Response Plan and Incident Record Log Templates	 Appendix I - Data Breach Response Plan
Appendix II	Notification to the Commission	 Appendix II Notification to the Commission
Appendix III	Notification to Affected Individuals	 Appendix III Notification to Affected Individuals
Appendix IV	Cyber Incident Response Checklist	 Appendix IV Cyber Incident Response Checklist
Appendix V	Post-breach Evaluation	 APPENDIX V Post Breach Evaluation.doc