STRATEQ GROUP DATA BREACH MANAGEMENT POLICY

Include In Countries Local Guides

PROPRIETARY NOTICE

This Group Data Breach Management Policy is the property of Strateq. It must not be reproduced in whole or on part or otherwise disclosed without prior written consent from Strateq Management.

This official controlled copy of Group Data Breach Management Policy is digitally signed PDF document held within Strateq network and visible to all authorized users.

All printed copies and all electronic copies and versions, except the one described above, are considered uncontrolled copies which should be used for reference and need to know basis only.

The policy is approved and duly signed by

Datuk Tan Seng Kit (May 8, 2025 17:11 GMT+8)

Datuk Tan Seng Kit
Group Managing Director

JUNE 1, 2025

STRATEQ GROUP OF COMPANIES

Contents

1 INTRODUCTION 2
1.1 OBJECTIVE 2
1.2 POLICY COMPLIANCE 2
1.3 APPLICABLE OF LOCAL LAWS 2
2 POLICY STANDARDS 2
2.1 DATA BREACH MANAGEMENT TEAM 2
2.2 DATA BREACH RESPONSE PROCEDURE 2
2.3 LOCAL GUIDELINES 4
APPENDIX 1: DATA INCIDENT REPORT TEMPLATE – FOR MALAYSIA 7
APPENDIX 2: DATA INCIDENT REPORT TEMPLATE – FOR IN-COUNTRIES (EXCEPT MALAYSIA) 11
APPENDIX 3: DATA BREACH RESPONSE PROCEDURE 13
CHANGE HISTORY 14

1 Introduction

1.1 Objective

Strateq is committed to compliance with data protection laws. This Data Breach Management Policy ("Policy") forms part of Strateq's data protection compliance program and supplements the Group Data Protection Policy.

This Policy applies to the Strateq group of companies worldwide ("Strateq"). All personnel must comply with this Policy when handling data breach incidents involving personal data in connection with Strateq's business and operations.

1.2 Policy Compliance

Laws around the world impose obligations on Strateq to protect and lawfully use personal data that we process in connection with our business. Failing to comply with such laws may expose Strateq to financial penalties, as well as damage to our reputation and customer confidence. Therefore, personal data must at all times be handled in accordance with this Policy and other related policies, procedures, notices, and standards which may be implemented from time to time. Personnel who fail to comply with this Policy may be subject to disciplinary action, up to and including dismissal.

1.3 Applicable of Local Laws

This Policy is based on generally accepted data protection principles and is intended to supplement local laws. Where local laws conflict with or impose stricter requirements than those set out under this Policy, such local laws will take precedence; in such case, the relevant Strateq entity should work with the Group Data Protection Officer ("DPO") to find a practical solution that meets the purpose of this Policy. Where local laws do not govern the processing of personal data, this Policy must still be complied with.

2 Policy Standards

2.1 Data Breach Management Team

Strateq shall appoint a Data Breach Management Team ("DBMT") to address and handle any known, suspected, or potential threat to the security of personal data, including unauthorized access, acquisition, disclosure, or use of the personal data ("Data Breach Incidents") in the manner described in this Policy. The DBMT shall follow the Business Continuity Management structure, with DPO becomes the chair and convener of DBMT.

2.2 Data Breach Response Procedure

Step 1 - Notify DPO
Any employee who discovers, suspects, or otherwise learns about Data Breach Incident must immediately report the issue to the DPO.

Step 2 - Initial assessment by DPO
The DPO shall obtain as much information as is readily available about the Data Breach Incident and decide promptly (usually within 24 hours) as to whether, based on available information, a reasonable or credible basis exists to believe that a Data Breach Incident has occurred.

If a reasonable or credible basis exists, the DPO shall (i) immediately notify and convene the DBMT, and (ii) based on the available information, conduct an initial assessment of the severity of the Data Breach Incident using the following criteria:

a) Type and volume of personal data involved e.g. a Data Breach Incident involving sensitive personal data and financial data would be more severe as compared to simple contact data.
b) Ease of identification i.e. how easy it will be for a party who has access to the set of data to unequivocally match them to a certain person.
c) Circumstances of the breach i.e. whether there is malicious intent and the context of the loss of confidentiality, availability and integrity.

If no reasonable or credible basis exists, the DPO completes an internal report that includes (i) the identity of the reporting party (or parties) if provided, (ii) a description of the circumstances of the reported Data Breach Incident, and (iii) an explanation of why the DPO determined that there was no reasonable or credible basis to believe there might be or have been a Data Breach Incident.

Step 3 - Investigation, mitigation and response

The DBMT is responsible for investigating and gathering information regarding the scope of the suspected Data Breach Incident, including, as appropriate:

a) when and how the suspected Data Breach Incident occurred and when it was discovered;
b) the categories of personal data and other data that may be at risk of compromise;
c) the risks of potential abuse or harm; and
d) who is aware of the suspected Data Breach Incident inside and outside of Strateq.

The DBMT is also responsible for the following:

a) Taking appropriate action to preserve any relevant information and evidence.
b) If a persistent or ongoing threat (e.g. a hacker or virus on Strateq's information systems) occurs, ensuring that appropriate IT / Information Security personnel determine appropriate actions to take to secure and isolate the threat so that it does not continue to cause harm to Strateq's technical environment (while still preserving evidence as mentioned above).
c) Considering applicable insurance policies taken out by Strateq to determine whether such policies mandate any procedures for responding to suspected Data Breach Incidents, or the engagement of certain forensic providers or external counsel.
d) Developing a response strategy for inquiries by the press, the government, or any other party. In most circumstances, inquiries should be directed to the Legal Department, which will work in conjunction with Public Relations to decide on how to respond (if at all) to such inquiries

The DBMT shall work with other departments to ensure every suspected Data Breach Incident is kept confidential until a decision regarding notification or disclosure is made and shall also keep the number of employees who know about the Data Breach Incident as limited as possible.

Step 4 - Notification / reporting requirements

The DBMT must, in parallel with step (3) above, determine (with reference to the Local Guidelines below):

a) whether the Data Breach Incident triggers contractual, statutory or other security breach notification obligations;
b) the timeframe within which such requirements must be fulfilled; and
c) if there are specific requirements regarding the content of the notifications (note that some jurisdictions have prescribed data reporting forms).

Step 5 - Corrective measures

The DBMT shall determine what technical and organizational security measures are necessary to prevent similar Data Breach Incidents in the future, including policies, awareness training, procedures for employees. The DBMT shall evaluate third-party relationships that might have been involved in the Data Breach Incident and take appropriate action e.g., contractual changes, alterations in procedures and/or training, improvements in security measures, moving to a different vendor, etc.

Step 6 - Documentation and reports

The DBMT shall maintain documentation of the steps that it takes from the time in which the Data Breach Incident is discovered through notice and remediation.

Specifically, the DPO shall prepare a report on the Data Breach Incident including the response process and control measures ("Data Incident Report"), as well as any amendments or improvements required to enhance the same. A template for the Data Incident Report is provided in Appendix 1.

A flowchart outlining steps 1-6 above is set out in Appendix 2.

2.3 Local Guidelines

Additional local law requirements may apply for Data Breach Incidents as below.

Jurisdiction	Local Law Requirements
Malaysia	Follow Circular of the Personal Data Protection Commissioner Number 2 Year 2025 Data Breach Notification.
United States	Please also refer to Strateq's HIPAA Policies (including the Policy on Security Incident Procedures and the Breach Notification Policy). In the event of any inconsistency between this Data Breach Management Policy and Strateq's HIPAA Policies, the latter will prevail.
China	None.
Hong Kong	Hong Kong has a voluntary data breach notification requirement. The DBMT should determine whether to report breaches to the Privacy Commissioner and/or data subjects where a real risk of harm is reasonably foreseeable in a data breach. Where a decision is made to notify the Privacy Commissioner and/or data subjects, the notification should include the following information: a) A general description of what occurred; b) The date and time of the breach, and its duration, if applicable; c) The date and time the breach was discovered; d) The source of the breach (either the data user itself or the third party that processed the personal data on its behalf); e) A list of the types of personal data involved; f) An assessment of the risk of harm (such as identity theft or fraud) as a result of the breach; g) A description of the measures already taken or to be taken to prevent further loss, unauthorized access to or leakage of the personal data; h) The contact information of a department or an individual designated by the data users within the organization for affected data subjects to obtain more information and assistance; and

Jurisdiction	Local Law Requirements
	i) Whether law enforcement agencies, the Privacy Commissioner and such other parties have been notified. Where the DBMT determines that a data breach should be reported to the Privacy Commissioner, the following form should be used.
Singapore	There are obligations pursuant to the Personal Data Protection Act 2012 to notify: a) the Personal Data Protection Commissioner (PDPC), as soon as is practicable, but in any case no later than 3 calendar days from the day that Strateq determines that a data breach is a notifiable data breach; b) affected individuals whose personal data is affected by a data breach as soon as practicable, at the same time or after notifying the PDPC (but there are some exceptions); and/or c) the organization or public agency that a data intermediary is processing personal data on behalf of (if Strateq is a data intermediary) without undue delay from the time it has credible grounds to believe that the data breach has occurred. A data breach in relation to personal data, means the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or 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. A data breach is notifiable if the data breach: (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale. While there may be varying circumstances that would affect the time taken to establish the facts of a data breach and to determine whether it is notifiable, the DBMT should take reasonable and expeditious steps to assess whether a data breach is notifiable, and this should generally be done within 30 calendar days from the date Strateq has grounds to believe that a data breach has occurred. Do note that data processors are not obliged to conduct an assessment of the data breach.

<table>
<tr>
<td>Thailand</td>
<td>Data Breach Incidents notification obligations that Strateq as a data user will need to comply pursuant to the applicable data protection laws are as follows:
<table>
<tr><th>Obligations</th><th>What</th><th>When</th><th>Timeframe</th></tr>
<tr><td>Duty to notify to the Office of the Personal Data Protection Committee</td><td>Notify the occurrence of the Data Breach Incidents, and other details as required by the sub-regulation on Data Breach Incidents notification - no such sub-regulation to date.</td><td>When the occurrence of the Data Breach Incidents is likely to result in a risk to the rights and freedoms of the persons.</td><td>Without delay and within 72 hours after having become aware of the Data Breach Incidents.</td></tr>
<tr><td>(2) Duty to notify to the data subject</td><td>Notify the occurrence of the Data Breach Incidents and remedial measures, and other details as required by the sub-regulation on Data Breach Incidents notification - no such sub-regulation to date.</td><td>When the occurrence of the Data Breach Incidents is likely to result in a high risk to the rights and freedoms of the persons.</td><td>Without delay.</td></tr>
</table>
Remarks: The exception to the Data Breach Incidents notification obligations and means/method for notifying the Data Breach Incidents will be prescribed by the Personal Data Protection Committee - no such sub-regulation on Data Breach Incidents notification to date.</td>
</tr>
</table>

Appendix 1: Data Incident Report Template – For Malaysia

Submission of notification:

PERSONAL DATA PROTECTION COMMISSIONER
8th Floor, Galeria PjH, Jalan P4W
Persiaran Perdana, Presint 4
62100 W.P Putrajaya
or via email: dbnpdp@pdp.gov.my

PARTICULARS OF DATA CONTROLLER	
ORGANIZATION:	
ADDRESS:	
CONTACT PERSON DETAILS:	
NAME:	
DESIGNATION:	
TELEPHONE:	
EMAIL:	
DATE OF REPORT:	
SIGNATURE:	

SECTION A: BASIC INFORMATION	
1. Is this a new notification or an update to a previous notification that has been submitted to the Commissioner?	
☐	New notification
☐	Update. Please indicate the reference number of the original notification:
2 If this is a new notification, are you submitting it within the 72 hours after becoming aware of the personal data breach?	
☐	Yes
☐	No. Please provide the reason(s) for the delay with supporting evidence:

SECTION B: DETAILS OF THE PERSONAL DATA BREACH	
3 When did your organization become aware of the personal data breach? *[(Please include the date and time of when your organization became aware of the breach)*	
Date:	**Time:**
4 How did your organization become aware of the personal data breach? *(Please provide a brief explanation of how your organization detected the personal data breach)*	
5 How was personal data affected or compromised? *(Select all that apply)*	
☐	Data was disclosed to unintended parties

☐	Data was lost
☐	Data was temporarily unavailable
☐	Data was exfiltrated / stolen
☐	Unauthorised access of personal data
☐	Others:

6 What is the actual or suspected cause of the incident?
(Select only one)

☐	Cyber incident
☐	Human error
☐	System error
☐	Theft / misuse of information by malicious actors
☐	Others:

7 How was the actual cause of the above incident identified?
(Please specify)

8 Which system or application was affected in this personal data breach incident?
(Please specify)

9 Where is the storage location of the personal data affected by this personal data breach?

☐	Malaysia
☐	Other jurisdiction (Please specify)

10 What is the status of the personal data breach incident?

☐	In Progress
☐	Rectified / Contained

11 Are there any other parties affected by the personal data breach (e.g., other data controllers or data processors)?

☐	No
☐	Yes. Please list out these parties:

SECTION C: DETAILS OF COMPROMISED DATA

12 What types of personal data were compromised?

13	**Number of data subjects affected or potentially affected?**
14	**Does this personal data breach only affect data subjects who are Malaysian citizens?**
☐	Yes.
☐	No. The breach also affects data subjects in the following jurisdictions:
15	**What harm or risks may result from the personal data breach affecting data subjects?**
☐	Physical harm to threat to safety
☐	Financial loss
☐	Identity theft or fraud
☐	Misuse of data for unlawful purposes
☐	Data contains sensitive data
☐	Data contains financial information
☐	No potential harm to data subjects
☐	Others (Please specify)
SECTION D: CONTAINMENT AND RECOVERY ACTIONS	
16	**What actions have been or will be taken to contain and mitigate the harm or risks arising from the breach?**
17	**What actions have been or will be taken to contain and mitigate the harm or risks arising from the breach?**
SECTION E: COMMUNICATION AND NOTIFICATION	
18	**Have you communicated or directly interacted with the suspected or actual threat actor?**
☐	Yes
☐	No
☐	Not applicable. There are no threat actor is involved.
19	**Have you notified or will you notify any local or foreign regulatory bodies regarding this personal data breach?**
☐	Yes. These regulatory bodies include:
☐	No
20	**Have you notified the affected data subjects about the personal data breach?**

☐	Yes. (Please attach a copy or sample of the notification provided)
☐	No, but we intend to notify the affected data subjects.
☐	No. We do not intend to notify the affected data subjects. (Please provide justifications)
21	**If you answered "Yes" to Question 20, how was the notification to the affected data subjects made?**
☐	Direct and individual notification (e.g., via email to affected data subjects).
☐	Public announcement (e.g., social media and press release).
SECTION F: OTHERS	
22	**Is there any additional information related to this personal data breach?**

Appendix 2: Data Incident Report Template – For In-Countries (Except Malaysia)

GROUP DATA PROTECTION OFFICER (DPO) DETAILS:	
ORGANIZATION:	
ADDRESS:	
NAME:	
DESIGNATION:	
TELEPHONE:	
EMAIL:	
DATE OF REPORT:	
SIGNATURE:	
DATA BREACH INCIDENT DETAILS:	
DATE & TIME OR PERIOD OF INCIDENT/ DATA BREACH DISCOVERED:	
DESCRIPTION OF DATA BREACH: *[personal data breach means any breach of personal data, loss of personal data, misuse of personal data or unauthorized access of personal data]*	
TYPE OF PERSONAL DATA INVOLVED: *[please specify whether this is direct personal data, indirect personal data, pseudonymized personal data, special personal data]*	
METHOD OF IDENTIFICATION AND SUSPECTED CAUSE OF THE BREACH:	
CATEGORIES & NUMBER OF DATA SUBJECTS AFFECTED:	
CATEGORIES OF PERSONAL DATA RECORDS AFFECTED:	
THIRD PARTIES INVOLVED (IF ANY, PLEASE NAME ALL VENDORS):	
PERSONAL DATA SYSTEM INVOLVED IN THE BREACH:	
POSSIBLE CONSEQUENCES OF THE BREACH:	
CHRONOLOGY EVENTS OF THE DATA BREACH: *[please attach the full report]*	
IMMEDIATE ACTION TAKEN TO CONTAIN/ MITIGATE BREACH:	
MEASURES TAKEN/ PROPOSED TO ADDRESS AFFECTED DATA SUBJECTS:	

OUTCOME OF INVESTIGATION:

[describe investigation findings and enclose supporting documents, if any]

CORRECTIVE ACTIONS:

NO	CORRECTIVE ACTIONS	TIMELINE	OWNER

DATA BREACH NOTIFICATION TO THE COMMISSION:

☐	**Within 72 hours of data breach discovered**
☐	**After 72 hours of data breach discovered.** **Reason for late notification to the commission & please attach all supporting documents:**
☐	**Full report within 30 days from the initial notification to the Commission** *[please attach the full report]*

DATA BREACH NOTIFICATIONS/ REPORT TO THE DATA SUBJECT:

☐	Yes. Completed within 7 days upon notification to the Commission.		
	Media:	☐	Public notice through mass media
		☐	Letter/ Email
		☐	Direct Call/ WhatsApp/ SMS
		☐	Others: Please specify.
☐	No. Reason for late notification to the data subjects:		

Insert details of data breach notifications to data subjects. You must include the following:

- Details of the breach
- Possible consequences
- Actions taken or proposed to mitigate the breach
- Detailed steps to be taken to minimize risk
- Contact details of the data protection officer for further information

[please attach the full notification]

DPO ENDORSEMENT:

SIGNATURE:	
DATE:	

Appendix 3: Data Breach Response Procedure

Step 01: Notify

Employee(s) to notify DPO upon becoming aware if Data Breach Incident (example: any known/ suspected/ potential threat to the security of personal data)

Step 02: Initial Assessment by DPO

DPO to conduct initial assessment and determine whether a Data Breach Incident has occurred.
If YES: DPO shall assess the severity of the incident and convene DBMT to investigate and develop response.
If NO: DPO shall complete an internal report documenting basis for decision.

Step 03: Investigation, Mitigation and Response

DBMT shall investigate, implement mitigating measures and develop appropriate response (example: preserve evidence, secure and isolate threat, consider applicable insurance policies, develop response strategy for inquiries to/ by third parties and ensure confidentiality)

Step 04: Notification and Reporting Requirements

DBMT must, in parallel with step 03, determine applicable notification/ reporting requirements. (example: whether contractual, statutory or other security breach notification obligations are triggered, timeline in fulfilling such requirements. Content of the notifications.)

Step 05: Corrective Measures

DBMT shall determine corrective measures to remediate and prevent similar incidents in the future.
(example: identify appropriate technical and organization security measures such as policies, awareness training and procedures for employees, evaluate third party relationship and etc)

Step 06: Documentation and Report

DBMT shall maintain documentation of all steps taken above. DPO shall prepare a Data Incident Report.

End of Personal Data Breach Management Policy

Change History

Date	Old Version	Page(s)/ Section(s)	Change Description	Changed By	New Version
01 Jan 2025	1.0	All pages	Update all sections in the Personal Data Breach Management Protection Policy.	DPO	2025-001
01 Jun 2025	2025-002	Sec 2.3 & Appendix 1	Update local guidelines for Malaysia jurisdiction. Update Data Incident Report Template for Malaysia and all other In Countries jurisdiction.	DPO	2025-002