NUS DATA MANAGEMENT

DATA INCIDENT REPORT

REPORTING LOSS OR LEAKAGE OF UNIVERSITY DATA INVOLVING PERSONAL DATA

AND BUSINESS CONTACT INFORMATION

Important Notes:

1. Please use this Form to report data breaches to the Personal Data Protection team ("PDP Team") in the Office of Risk Management and Compliance if there are data breaches involving personal data ("PD") including Business Contact Information (BCI) (i.e., Details of individuals required for business purposes.)

   Refer to the NUS Data Management Policy (DMP) for more details.
2. To be completed by Data Users and submitted to DPO at dpo@nus.edu.sg
3. Please do not reference any data subjects by name in this report.
4. Circulation of this report must be restricted to those involved in investigating/evaluating the incident.
5. Timelines:
   - Containment of the data breach: As soon as possible and in any event no later than **one (1) calendar** day after the Data Steward/HOD first becomes aware of the data breach.
   - Completion of this Data Breach Report and submission to DPO at dpo@nus.edu.sg Within **one (1) calendar** day after the Data Steward/HOD first becomes aware of the data breach.
   - All additional information/updates related to the data breach must be reported to DPO using this Form **within one (1) working day** after the Data Steward/HOD first become aware of the said additional information.

Section A: Case Information

1a.	1a. Does this data breach involve PD? * ○ YES ○ NO If no; there is no need to report to the NUS PDP Team. You would however need to report to NUS IT for data breaches that do not involve PD using the on-line IT security Form at https://forms.office.com/pages/responsepage.aspx?id=Xu-lWwkxd06Fvc_rDTR-gtCIKGO2DKhNkGJ8fF10JrtUNjRORkNSRlMwTzQzQzNDMTNYUDJaTFZIWCQlQCN0PWcu&route=shorturl

1b.	1b. Does the personal data relate to human subjects research? * ○ Yes ○ No If “Yes” : Please ensure that NUS IRB (irb@nus.edu.sg) reporting requirements are followed.
2.	2. Date of occurrence of data breach incident: * **Date:** Select Date **Time:** Select Time
3.	3. When did the Reporting Personal first become aware of the data breach: * **Date:** Select Date **Time:** Select Time
4.	4. When did the Data Steward/HOD/RO first become aware of the data breach: * **Date:** Select Date **Time:** Select Time

Section B: Data Breach Report involving Personal Data

1. Please describe in detail the nature and details of the data breach: *

Category	Details	Response
Nature and Details of the Data Breach	Describe what happened and the extent of the breach.	
Personal Data (PD) Leaked	List the types of PD and BCI that were exposed.	
Purpose/Intent of the PD	Explain why this data was collected and its intended use.	

Category	Details	Response
Discovery of the Data Breach	Identify who first discovered the breach and how they found it.	
Details of the Breach	Provide information on why and how the breach occurred.	
Personnel Involved	Mention any individuals or teams involved in the incident.	
Other Relevant Information	Include any additional details that are important to note.	

2. Please indicate which of the following caused/contributed to the data breach: *

□ **PDPA Issues:**

□ No notification □ No consent □ Inaccuracy at collection/processing □ Inadequate protection

□ Unintended disclosure or transfer □ Unsecured disposal/storage

□ **IT/Technical Issues:**

□ Software processing error □ Unauthorized access/download by staff

□ Lack of access protection on website/apps

□ Human Error: Mistakes made by employees

□ Untrained/New Staff: Lack of proper training

□ Non-compliance: Not following NUS policies

□ Vendor/Provider Errors: Mistakes by vendors or software developers

□ **Malicious Activities:**

□ Internal threats □ External threats

□ Others: Specify any other causes

3. Please provide the following details about the impacted data *

Data Category	Specific Data items	How many records were impacted?	Action
Choose a category ⌄	Select category first ⌄	Example: 20	🗑
Choose a category ⌄	Select category first ⌄	Example: 20	🗑
Choose a category ⌄	Select category first ⌄	Example: 20	🗑
Choose a category ⌄	Select category first ⌄	Example: 20	🗑
Choose a category ⌄	Select category first ⌄	Example: 20	🗑

Add Row

Note: Breach of records >= 500 must be reported to PDPC within 3 calendar days once the reporting office/DPO is aware of the breach.

4. Please list the IT systems, network, servers, databases, platforms, mobile applications etc. etc. that were involved in this data breach if any *

□ N.A.: physical records

□ **Servers:**

□ Internal servers (within the company) □ External servers (outside the company)

□ **Storage Systems:**

□ File storage (e.g., network drives, IaaS (Infrastructure as a Service), cloud storage)

□ Backup systems (e.g., backup servers, cloud backups)

□ **Networks:**

□ Internal networks (company's private network) □ External networks (public or partner networks)

□ **Platforms:**

□ Web platforms (websites and web apps)

□ Application platforms (Software applications e.g., (SaaS (Software as a Service) such as Microsoft Office Suite, Zoom and SAP, etc)

□ **Mobile Applications:**

□ iOS apps (Apple devices) □ Android apps (Google devices)

□ **Websites:**

□ NUS websites (official NUS sites) □ Client portals (customer access sites)

□ **Email Systems:**

□ Internal email systems (company email) □ External email systems (third-party email services)

5. Is this data breach a new incident, or has it happened before in your department or with the same staff/system/vendor? *

○ New incident ○ Repeated incident ○ Same staff/system/vendor was involved in a previous incident

6. Where is/are the affected database(s)/server(s) holding the personal data involved in this incident located? *

Singapore

7. Number of Individuals Affected: *

8. In your assessment would this data breach have a significant negative impact on NUS and/or the Data Subjects? *

Risk Factor	Question	Response
Reportable to PDPC	Are 500 or more records impacted?	○ Yes ○ No
	Is there potential harm to data subjects (e.g., credit card details leaked)?	○ Yes ○ No
Complaints	Is there a possibility of data subjects lodging a complaint to PDPC?	○ Yes ○ No
Operational Disruption	Will the breach disrupt operations for one work day or more?	○ Yes ○ No
Reputation Damage	Could this breach damage the university's reputation if made public?	○ Yes ○ No
Public Accessibility Duration	Was the compromised data publicly accessible for more than 24 hours?	○ Yes ○ No

Risk Factor	Question	Response
Third party involvement	Were there any other organisations affected?	○ Yes ○ No
Affected individuals	Are there any Singapore-based Individuals affected?	○ Yes ○ No

Section C: Remediation & Corrective Actions

1. What actions have you taken immediately to contain harm or mitigate the impact of the data breach to the individuals whose PD was leaked (Data Subjects) as well as NUS? *

Action	Description	Response
Isolated Affected Systems	Disconnected compromised systems from the network to prevent further damage.	○ Yes ○ No
Changed Access Credentials	Reset passwords and access keys for affected accounts.	○ Yes ○ No
Notified Affected Individuals	Informed individuals whose data was compromised and the steps being taken.	○ Yes ○ No
Removed Public Data	Removed leaked data from public websites.	○ Yes ○ No
Engaged Forensic Experts	Hired experts to investigate the breach and preserve evidence.	○ Yes ○ No
Secured Physical Areas	Locked and secured physical areas related to the breach.	○ Yes ○ No
Updated Software and Systems	Applied patches and updates to software and systems to fix vulnerabilities.	○ Yes ○ No
Conducted Staff Training	Provided training to staff on data protection and breach response.	○ Yes ○ No
Reviewed and Updated Internal Process	Reviewed and updated internal data protection process.	○ Yes ○ No
Monitored for Further Breaches	Continuously monitored systems for signs of further breaches.	○ Yes ○ No

Action	Description	Response
Verified Data Integrity	Ensured the integrity and accuracy of data by cross-checking with the data subject affected.	○ Yes ○ No
Provided Support to Affected Individuals	Offered assistance to individuals impacted by the breach (e.g., credit monitoring).	○ Yes ○ No

2. What follow-up corrective and prevention actions would the Department be taking to prevent future occurrence of such data breach incidents: *

Corrective Actions [Definition: Steps to address and fix the immediate effects of a data breach, containing the breach and mitigating its impact]

Action	Action Owner	Target Completion Date	Status	Action
[Describe Correctiv	[Name/Role]	Select Date	In Progress ⌄	🗑

Add Corrective Action

Preventive Actions [Definition: Measures to prevent future data breaches, focusing on strengthening security, improving processes, and educating staff to reduce risks.]

Action	Action Owner	Target Completion Date	Status	Action
[Describe Preventiv	[Name/Role]	Select Date	In Progress ⌄	🗑

Add Preventive Action

Section D: Declaration by Reporting Personnel

Status of investigation by Department: *	○ **Initiation:** The investigation has just started. ○ **Ongoing:** The investigation is actively being conducted. ○ **Pending:** Awaiting further information or actions. ○ **Completed:** The investigation has concluded, and findings are available.

Date of completion of investigation by Department:	Select Date

Contact Information

Name *	
Email *	

Declarations: *

- □ I confirm the information stated herein is complete, true and accurate at the time of submission of this Report.
- □ My Head of Department /Data Steward have been informed of the data incident and have reviewed this incident report.
- □ If there are any changes in circumstances or updates in relation to the data breach incident, I will inform DPO immediately with an update of this report as soon as I am aware of the same.
- □ The Department affirms that all supporting evidence of the corrective and preventive actions taken will be submitted to dpo@nus.edu.sg for verification and record-keeping.

Save as Draft Submit Report Download PDF Download Template PDF

Please ensure all required fields are completed before submitting.

Disclaimer: The views and opinions expressed herein are those of the author(s) and do not represent the views and opinions of the National University of Singapore or any of its subsidiaries or affiliates.

Privacy Notice