***NUS DATA MANAGEMENT***

**DATA BREACH REPORT**

**REPORTING LOSS OR LEAKAGE OF UNIVERSITY DATA INVOLVING PERSONAL DATA**

**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”).

Refer to the NUS [Data Management Policy (DMP)](https://share.nus.edu.sg/opc/NUSpolicy/Shared%20Documents/NUS-Data-Mgt-Policy%281%29.pdf) for more details.

1. To be completed by Data Users and submitted to DPO at dpo@nus.edu.sg
2. Please do not reference any data subjects by name in this report.
3. Circulation of this such report must be restricted to those involved in investigating/evaluating the incident.
4. 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**

|  |  |
| --- | --- |
| 1. | Does this data breach involve PD? 🞏YES 🞏 NOIf 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://nusit.nus.edu.sg/its/cceforms/i-want-to/report-an-incident/> |
| 2. | Date of occurrence of data breach incident:  |
| 3. | When did the Reporting Personal first become aware of the data breach: |
| 4. | When did the Data Steward/HOD/RO first become aware of the data breach: |

**Section B: Data Breach Report involving Personal Data**

|  |  |
| --- | --- |
|  | Please describe in detail the nature and details of the data breach: * PD that was leaked?:
* Purpose/Intent of the PD?:
* Who first discovered the data breach? How?:
* Details of why and how the data breach occurred?:
* Personnel involved?:
* Others:
 |
|  | Please indicate which of the following caused/contributed to the data breach:🞏PDPA No notification, No consent, Inaccuracy at collection; Inaccuracy in processing, Inadequate protection; No verification/Errors at transfer/disclosure of PD; Unsecured disposal of PD; Unsecured storage of PD etc.🞏IT/Technical systems – software processing error; unauthorized access/download by staff; lack of access protection at website/mobile apps portal🞏Human Error 🞏Untrained staff /new staff🞏Non-compliance with NUS DMP/ NUS IT Policy/NUS Personal Data Protection Policies & Procedures🞏Error by vendor/CSP Provider/Software developer (Data Intermediaries)🞏Malicious activities by internal🞏Malicious activities by external parties🞏 Others: Please specify |
|  | PD ImpactedPlease indicate NUSData Classification, Data Type and number of PD records leaked or impacted (Note: breach of records >=500 has to be reported to PDPC within 3 calendar days once reporting office /DPO is aware of the breach) | Data Classification/Categorye.g. NUS Confidential (students’ record) | Data Type – e.g. Name/NRIC/medical records/email address | No of Records impacted e.g. 10 persons |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  | Please list the IT systems, network, servers, databases, platforms, mobile applications etc. etc. that were involved in this data breach if any  |
|  | Is this data breach a new incident? Has it happened before in your department or has the same staff/system or vendor (data intermediary) caused a date breach incident previously? |
| 6. | In your assessment would this data breach have a significant negative impact on NUS and/or the Data Subjects? Impact can be assessed on the basis of, *inter alia*:* Reportable to PDPC:

(i)Significant scale: ≥=500 records impacted(ii)Potential harm caused to data subject e.g. credit card detail leaked* Possibility of data subjects lodging a complaint to PDPC
* Disruption to operations for one work day or more
* Damage to university reputation if this data breach is made public
* Duration for which the compromised PD was publicly accessible (leaked PD posted at public websites)
 |

**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? |
| 2. | What follow-up corrective and prevention actions would the Department be taking to prevent future occurrence of such data breach incidents: Corrective Actions (Action Owner, Target Completion Date, Status)Preventive Actions(Action Owner, Target Completion Date, Status) |

**Section D: Declaration by Reporting Personnel / Data Steward / HOD**

|  |  |
| --- | --- |
| Status of investigation by Department: |  |
| Date of completion of investigation by Department:  |  |

I confirm the information stated herein is complete, true and accurate at the time of submission of this 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.

Signature of Reporting Personnel:

Name of Reporting Personnel:

Designation:

Department:

Date:

Signature of HOD/Data Steward:

Name of HOD/Data Steward:

Designation:

Department:

Date:

**Section D: DPO Determination (to be completed by PDP Team)**

|  |
| --- |
| Case No.:  |
| Date of DPO Determination: |
| Date case closed by PDP Team: |
| This data breach event is reportable to PDPC: 🞏YES 🞏 NO Basis for assessment: |
| Feedback for further improvement to prevent future occurrence of data breach |
| Any other comments  |

|  |  |
| --- | --- |
|  |  |