|  |  |  |
| --- | --- | --- |
| Incident Details | | |
| Data and time of the data breach or report of breach: |  | |
| Location of the data breach: |  | |
| Was anyone informed about the breach? Who?  Please include whether the party informed took any actions or remediation steps and ensure evidence of any such actions is saved. |  | |
| What mitigation strategies were implemented immediately after the breach (48 hours):  Please note: Keep evidence including notifications via Service Now, SRM or other systems. |  | |
| Description of the data breach (i.e. what happened, what types of personal information were involved, how many records were disclosed or how many individuals were impacted). Was the information commercial in confidence, legally privileged or communications between the Senior executive or Health Professionals?  Data classification if any (restricted/Confidential/internal). |  | |
| How was the breach detected: |  | |
| Threat actor: External/ Internal/ Vendor (who appears to be responsible for the breach).  Or how did the breach occur e.g. human error, loss of files etc. |  | |
| Were individual identities apparent or reasonably ascertainable? |  | |
| Is the personal information adequately encrypted, anonymised, or otherwise not easily accessible? |  | |
| What systems (e.g. devices, email accounts, databases, worksites, etc.) were affected by the breach if known?  Or  What physical information was involved in the breach (e.g. hard copy files, notes, patient files, class lists etc.)? |  | |
| Interim assessment of harm include documentation on why decisions were made: |  | |
| Intermediate mitigation strategies – after initial investigation what additional mitigation strategies were implemented, if any: e.g. whole staff email change, notification to UNE community. |  | |
| Re assessment of harm: |  | |
| What actions were taken and when, (include when affected parties were notified, the dates and responsible party for the actions and the reasons behind them). |  | |
| Have the remedial actions successfully enabled the Business Continuity: Yes/No  If no please provide additional details. |  | |
| How long was the information accessible to unauthorised parties? |  | |
| Notes/Comments/remediation long term |  | |
| Attach any evidence of the breach, (e.g. computer logs, screenshots, emails etc.). Please include the Security Risk Matric category. | | |
| Signature: | | Date : |

***This form and all relevant attachments must be saved in Content Manager and access provided to the UNE Privacy officer.***