INFORMATION SECURITY AND PRIVACY INCIDENT NOTIFICATION FORM

Organisations that are subject to the Victorian Protective Data Security Standards (**VPDSS**) must notify OVIC of certain information security incidents. In addition, organisations that are subject to Part 3 of the PDP Act are encouraged to notify OVIC of incidents involving personal information that could cause harm to affected individuals.

**Any organisation that is subject to the PDP Act can therefore use this form to report incidents to OVIC, whether voluntarily or by obligation.**

SECTION 1: General Details

| **Field** | **Details (if known)** |
| --- | --- |
| Name of organisation |  |
| Contact name and position |  |
| Contact phone number |  |
| Contact email address |  |
| What happened? |  |
| When did it happen? |  |
| When did organisation become aware of it? |  |
| How did it happen? For example:* Who / what caused it?
* Malicious or accidental?
* Who accessed information in unauthorised manner?

*Please be as specific as possible. E.g. if referring to third party, name party or describe nature of party.* |  |
| Steps taken or proposed to contain incident. |  |
| Steps taken or proposed to prevent future incidents |  |

SECTION 2: PRIVACY (PERSONAL INFORMATION) INCIDENTS

Fill in the following fields if your incident relates to personal information. Please visit our website for further information on [managing the privacy impacts of a data breach.](https://ovic.vic.gov.au/privacy/managing-the-privacy-impacts-of-a-data-breach/)

| **Question** | **Details (if known)** |
| --- | --- |
| What personal information is involved? |  |
| What is the risk of harm to the affected individuals? * what type of harm?
* how serious?
* how likely?
 |  |
| Have affected individuals been notified about the incident?* if not, why?
* If so, how? What reactions?
 |  |

SECTION 3: INCIDENT NOTIFICATION SCHEME

Fill in the following fields ifthe affected organisation is subject to the VPDSS. If the organisation is not subject to the VPDSS, you may leave this section blank.

Please visit our website for further information on the [information security incident notification scheme](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/).

OVIC has entered a Memorandum of Understanding (MOU) with the Cyber Incident Response Service (CIRS) to exchange incident information, to reduce the reporting burden on organisations. If you require incident response assistance and would like OVIC to send the incident details to CIRS on your behalf, please check the following box: [ ]

| **Question** | **Details (select all that apply)** |
| --- | --- |
| What type of information was affected? | [ ]  Personal[ ]  Health[ ]  Financial[ ]  Policy[ ]  Legal[ ]  Operational[ ]  Critical Infrastructure[ ]  Law enforcement[ ]  Crime statistics[ ]  Other |
| What is the assessed Business Impact Level (BIL)[[1]](#footnote-2) of the affected information? | [ ]  BIL 1 - Minor[ ]  BIL 2 - Limited[ ]  BIL 3 - Major[ ]  BIL 4 - Serious |
| What was the information format? | [ ] Hard copy[ ] Electronic[ ] Verbal |
| What security attributes were affected? | [ ]  Confidentiality[ ]  Integrity[ ]  Availability |
| Was the incident primarily caused by people, process and/or technology control(s)? | [ ]  People[ ]  Process[ ]  Technology[ ]  No control(s) in place |
| Who did it? | [ ]  Internal personnel[ ]  Authorised third party[ ]  Other external[ ]  Other/ Unknown |
| What was the threat type? | [ ]  Accidental / Error[ ]  Failure[ ]  Malicious[ ]  Natural |
| Is the incident closed? | [ ]  Yes[ ]  No |
| Is the incident recorded in the organisation’s incident register? | [ ]  Yes[ ]  No |

1. Refer to your organisation’s BIL table or the [VPDSF BIL table](https://ovic.vic.gov.au/resource/vpdsf-bil-table-v2-1-november-2019/) to assess the potential business impact level. [↑](#footnote-ref-2)