# Information Security and Privacy Incident Notification Form

Any organisation that is subject to the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) can use this form to report incidents to OVIC, whether voluntarily or by obligation.

* This form should not be used by members of the public to report incidents, data breaches or alleged wrongdoing by VPS employees or organisations to OVIC.
* Individuals wishing to do so, should instead use [OVIC's Privacy Complaint Form](https://make-a-privacy-complaint.ovic.vic.gov.au/).

Organisations that are subject to:

* **Part 4** of the PDP Act and the Victorian Protective Data Security Standards (**VPDSS**) should notify OVIC of certain information security incidents, and
* **Part 3** of the PDP Act are encouraged to notify OVIC of incidents involving personal information that could cause harm to affected individuals.

**Send this completed form to** [**incidents@ovic.vic.gov.au**](mailto:incidents@ovic.vic.gov.au)

Collection of personal information

The incident notification form collects personal information including:

* your name
* position title
* organisation
* contact number, and
* email address for the purpose of follow up, research projects or activities set out in OVIC’s [Regulatory Action Policy](https://ovic.vic.gov.au/regulatory-approach/regulatory-action-policy/).

Where you provide personal information, OVIC may use it to provide you with return confirmation of receipt of your form, seek clarification on the contents of your form or report on any trends. If you do not provide the information requested in this form, it may limit OVIC’s ability to follow up with you. When submitting your form via email, we may be able to identify you from your email address.

OVIC will not disclose your personal information without your consent (e.g. where you request assistance from the Victorian Government Cyber Incident Response Service), except where required or authorised to do so by law. OVIC does publish de-identified information (or aggregated data) in our monitoring and assurance reports.

You may contact OVIC to request access to any personal information you have provided to us by emailing [enquiries@ovic.vic.gov.au](mailto:enquiries@ovic.vic.gov.au).

For further information on how OVIC handles personal information, please review our [privacy policy](https://ovic.vic.gov.au/resource/privacy-policy/).

**Important!** Do not include the personal information of any employees or individuals involved in, or impacted by, the incident. The only personal information requested is that of the organisation’s nominated contact representative which should be noted in the designated fields on this form.

## SECTION 1: General Details

| Field | Details (if known) |
| --- | --- |
| **Organisation details**  *This is the VPS organisation or contracted service provider you work for that is reporting an Incident to OVIC under VPDSS Element 9.010.* | |
| Name of organisation |  |
| Contact name and position of individual coordinating the incident on behalf of the above Organisation  *This is the person OVIC will contact and liaise with in relation to the incident.* |  |
| Contact phone number for the officer coordinating the incident to be used by OVIC |  |
| Contact email address  *Please ensure that the coordinating officer is aware, and care is taken to enter their email address correctly* |  |
| **Request for assistance**  Privacy  If you require privacy assistance (if the incident involves personal information), please check the box below:  *Yes, I would like privacy assistance*  Cyber Incident Response Service (CIRS)  If you require cyber incident response assistance and would like OVIC to send the incident details to CIRS[[1]](#footnote-1) on your behalf, please check the following box:  *Yes, I would like CIRS assistance* | |
| **Incident details** | |
| What happened? |  |
| When did it happen? |  |
| When did the organisation become aware of it? |  |
| How did it happen?  For example:   * What function, service or activity was being undertaken? * Who or what caused it? * Who or what party was involved (e.g. an external threat actor / employee / authorised contracted service provider)? * Was it malicious or accidental? * What was the extent of the access, disclosure or exposure?   *Please be as specific as possible, however do not include the names of individuals involved in, or impacted by the incident.* |  |
| What steps have been taken, or are proposed to be taken to contain the incident? |  |
| What steps will be taken or proposed to prevent future incidents? |  |
| Please note: Organisations can request a copy of the completed form submitted to OVIC by emailing [incidents@ovic.vic.gov.au](mailto:incidents@ovic.vic.gov.au) | |

## SECTION 2: Privacy (Personal Information) Incidents

If the incident you are notifying us about involves personal information, please fill in the following fields.

Under the PDP Act, personal information is information or an opinion that is about them, and that person could be reasonably identifiable. Examples of personal information may include names, contact details, financial details, signatures and more.

If you are not sure whether the information is personal information, fill out this section and OVIC will provide you with guidance. For more information on personal information see the [Guidelines to the Information Privacy Principles](https://ovic.vic.gov.au/book/key-concepts/#Personal_information).

If the incident you are notifying us about did not involve personal information, you may leave this section blank.

|  |  |
| --- | --- |
| Question | Details (if known) |
| What type of personal information is involved?  *Please do not include a copy of the actual personal information that was involved in the breach.*  *Instead, please nominate the types of personal information involved. For example, ‘first name and last name’ or ‘5 x personal email addresses.’* |  |
| 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, please explain how this position was reached. * If so, when did notification occur, by what method and were individuals informed of their right to make a privacy complaint? |  |

## SECTION 3: Incident Notification Scheme

*If the affected organisation is subject to the VPDSS, please fill in the following fields.*

*If the organisation is not subject to the VPDSS, you may leave this section blank.*

*Visit our website for further more information on the*[*information security incident notification scheme*](https://ovic.vic.gov.au/information-security/ovic-information-security-incident-notification-scheme/)*.*

| Question | Details (select all that apply) |
| --- | --- |
| What type of information was affected? | Personal  Health  Financial  Policy  Legal  Operational  Critical infrastructure or Essential service  Law enforcement  Crime statistics  Other |
| What is the assessed Business Impact Level (BIL) of the affected information?  *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.* | 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 |
| Where did the incident originate? | Internal personnel  Authorised third party  Other external  Other/ Unknown |
| What was the threat type? | Accidental/ Error  Failure  Malicious/ Intentional  Natural  Unknown |
| Is the incident closed? | Yes  No |
| Is the incident recorded in the organisation’s incident register? | Yes  No |

**Send this completed form to** [**incidents@ovic.vic.gov.au**](mailto:incidents@ovic.vic.gov.au)

1. OVIC has entered a Memorandum of Understanding (**MOU**) with the CIRS to exchange incident information to reduce the reporting burden on organisations. [↑](#footnote-ref-1)