|  |  |
| --- | --- |
| Question  | **Answer** |
| Information Security Incident Notification Scheme (ISINS) |
| Are there any repercussions for reporting/ not reporting information security incidents under Element 9.010 of the Victorian Protective Data Security Standards (**VPDSS**)? | Organisations must notify OVIC of an information security incident if it hits a Business Impact Level (BIL) of 2 or higher, no later than 30 days of identification. For more information on the Information Security Incident Notification Scheme refer to our [Information Sheet](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/).Organisations found to have deliberately withheld incident notification from OVIC may face repercussions in line with [OVIC’s Regulatory Action Plan](https://ovic.vic.gov.au/regulatory-action-policy/?highlight=regulatory%20action%20plan).  |
| Who reports information security incidents to OVIC? | OVIC will accept notification from anyone, however the information owner is best placed to notify OVIC of the information security incident.If the incident is first identified by a contracted service provider (CSP), the CSP should inform the information owner, who must notify OVIC of the incident. |
| Who do I report to? | The primary method to notify OVIC of information security incidents is via the OVIC incident notification form - <https://ovic.vic.gov.au/resource/ovic-incident-notification-form/>. OVIC also accepts information security incidents via:* Phone calls to OVIC’s Information Security Unit (**ISU**)
* OVIC’s Privacy and Guidance Team
* DPC’s Cyber Safety Unit (**CSU**)

Organisations are reminded to contact CSU for any cyber incidents that may require onsite coordination, as OVIC does not provide a 24/7 service.More information on how to report incidents to OVIC can be found on [OVIC’s website](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/). |
| Our incident requires us to notify multiple agencies. Who do I contact first? | If you have just identified a cyber security incident and you require immediate assistance in coordinating a response, the CSU run a 24-hour Cyber Incident Response Service (**CIRS**) and should be contacted as a priority.CSU are able to notify OVIC on your behalf, should you request this of them, or you can notify OVIC separately within 30-days of identifying the incident. |
| Will CSU automatically report to OVIC (and vice versa)? | CSU runs a confidential service and will only notify OVIC of information security incidents with your permission. They will, however, remind you of your obligation to notify OVIC of information security incidents under Element 9.010 of the VPDSS.Similarly, OVIC will only pass along details of the incident if you request it. Please check the relevant boxes on the [Information Security Incident Notification Form](https://ovic.vic.gov.au/resource/ovic-incident-notification-form/) if you require the OVIC Privacy team or assistance from CIRS team within the CSU. |
| Will OVIC share details of the breach with anyone else (e.g. a department or parent entity)? | OVIC will not share personal information captured in an incident notification without your consent. OVIC may however share de-identified outcomes of the analysis with Victorian government agencies and bodies, to help inform their own risk assessments. OVIC may also suggest that an organisation seek assistance/ advice from their Department or parent entity regarding the incident.If notification of the incident is received from a Third Party, OVIC may also follow up with the in-scope government organisation regarding the notification.  |
| Where will statistics from the Information Security Incident Notification Scheme (ISINS) be published? | Statistics from the ISINS will be published on the Victorian Information Security Network (**VISN**) on GovTEAMS and in OVIC’s annual report, and quarterly incident reports. |
| How often will you be publishing statistics from the ISINS? | We expect the first report on the ISINS will be published mid 2020 with subsequent reports published quarterly.  |
| What constitutes an information security incident (as opposed to a privacy breach, etc)? | The terms incident vs. breach are quite distinct and have different meanings.An **incident** refers to a compromise to the confidentiality, integrity and availability of information or information systems. Whereas a **breach** primarily focuses on a compromise to the confidentiality of information. For more information about, the [Information Security Incident Notification Scheme (ISINS)](https://ovic.vic.gov.au/data-protection/agency-reporting-obligations/incident-notification/) or [privacy breaches](https://ovic.vic.gov.au/privacy/for-agencies/responding-to-data-breaches/?highlight=privacy%20incident%20reporting), please see OVIC’s website. |
| An incident has occurred during or since the release of the ISINS which should have been reported to OVIC, however was not.Is there any flexibility with the 30-day deadline? | As the ISINS scheme is still relatively new, OVIC is providing organisations the opportunity to report ‘aged’ information security incidents that may have occurred since November 2019 and are of a BIL 2 or higher. This amnesty will for aged incidents at the end of June 2020.After June 2020, if organisations fail to notify OVIC within 30 days of identifying an incident, OVIC will still accept the notification and provide guidance if needed, but depending on the circumstances, may also decide that it is appropriate to activate its Regulatory Action Plan.For more information about OVIC’s [Regulatory Action Plan](https://ovic.vic.gov.au/regulatory-action-policy/?highlight=Regulatory%20action%20policy), please see OVIC’s website. |
| Is incident notification purely for statistical analysis? | Information security incident notification serves a number of purposes. Notifications provide OVIC important insight into, and oversight of, the information security threat environment across the Victorian government. This insight allows OVIC to tailor guidance material and develop resources to better assist organisations to meet these threats. OVIC will also provide reports back to organisations that will provide further insight into the broader risk landscape in which they are operating.  |
| What’s is OVIC’s advice on ‘highly’ sensitive material that has been compromised (e.g. personal/ financial documents such as Tax File Numbers)? | A range of different considerations come into play when managing an incident. These considerations include but are not limited to the nature of information and the potential consequences of the compromise.Different notifications may need to be made to regulating bodies, partnering entities and law enforcement agencies. Breaches that involve personal information that has been assessed as having the potential to cause serious harm to an individual, and meets the criteria for the [Notifiable Data Breaches Scheme](https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme/) (e.g. Tax File Numbers), should be reported to the Office of the Australian Information Commissioner’s (**OAIC**)Organisations that fall under Part 4 of the PDP Act (2014) are still required to notify OVIC of information security incidents that meet the notification threshold of a BIL of 2 or higher.  |
| How are you going to protect sensitive information in incident reports when transmitted and stored? | OVIC handles any information security incidents notification in accordance with its protective marking.Organisations submitting a notification to OVIC can apply a protective marking to the ‘Information Security Incident Notification Form’ by clicking on the dropdown fields at the top or bottom of each page.Alternatively, if specific handling requirements are required for the report, please contact the Information Security Unit (ISU) at OVIC by emailing security@ovic.vic.gov.au.  |
| 2020 Protective Data Security Plan (PDSP) |
| Can we apply for an extension on the Aug 2020 reporting deadline? | OVIC cannot provide extensions or exemptions as there are no legislative provisions to do so under the *Privacy and Data Protection Act 2014* (Vic)(**PDP Act**).We understand that in this current environment, certain programs of work supporting implementation of the VPDSS may be put on hold or will be noted as incomplete for this reporting period. Keep in mind the PDSP is simply a reflection of your organisation’s current information security program and future planning. If you are experiencing challenges, please list these on pg. 9 of the PDSP form. |
| Do you intend to provide feedback to organisations who have submitted a PDSP? | Yes - the ISU intend to provide ‘playback’ reports to organisation’s that submit a PDSP for the 2020 reporting cycle. These high-level reports will provide a contextual snapshot of the organisation’s PDSP against WoVG trends and common themes. It is estimated Playback reports be sent out by November 2020.Please note that organisations who submit PDSPs late may not receive a Playback report or may receive it later than organisations who submitted on time.Follow up meetings may also be arranged on request. |
| My agency is under resourced with limited capacity to complete the PDSP. What advice do you have for agencies like mine? | The PDSP is intended to be a point-in-time reflection of your organisation’s current information security program and future planning. The PDSP must be submitted to OVIC by August 31, 2020.To assist in the development of the PDSP, OVIC encourages engagement with all areas of the business, as subject matter experts in different business units that may be able to offer unique insights and understanding of the business context of certain Standards.OVIC also encourages organisations to plan well in advance, allowing enough time to submit their PDSP by the due date. The VPDSF assurance cycle is well defined, with - * submission of a PDSP is required every second year, and
* attestation is required every year.

If resource constraints are an issue, you may consider recording this in the ‘challenges and barriers’ section (pg.9 of the PDSP form). Your feedback will help OVIC understand where to target future advice. It may also highlight to your executive where potential resource constraints are within your organisation. |
| My parent organisation wants to do a Multi-org PDSP, but we would prefer to submit separately. What should I do? | Where possible, OVIC encourages organisations to submit a Single-Organisation PDSP. A Single-Organisation PDSP provides more detailed insight into the security plan of the specific organisation, rather than an aggregated view of the security activities of a combination of organisations. In some instances, an organisation may choose to assist with the submission of a consolidated PDSP (Multi-Organisation PDSP), based on a portfolio model or where organisations of a similar form of function choose to consolidate their reporting efforts. To find out more about this process, consider the information sheet – * [Multi-Organisation Protective Data Security Plan](https://ovic.vic.gov.au/wp-content/uploads/2020/02/Information-Sheet-Multiple-Organisation-Reporting-Process-V1.0.pdf)
* [Protective Data Security Plan submission workflow](https://ovic.vic.gov.au/wp-content/uploads/2020/02/Information-Sheet-Protective-Data-Security-Plan-Submission-Workflow.pdf)
 |
| What if two PDSPs are received from the same entity (e.g. via both Multi-Org and Single-Org)?  | If two PDSPs are received that reference the same organisation, OVIC will reference the Single-Organisation PDSP ahead of a Multi-Organisation PDSP. If the most current PDSP submitted exceeds the August 2020 deadline, OVIC will seek clarification from the organisation as to which one they would like to keep. |
| Not all of the Elements are applicable to my agency. Do I still need to fill them out on the PDSP? | If an element under the VPDSS is not applicable, the form provides an option to select ‘*Not Applicable’* for that element in the ‘Status’ column of Part B in the PDSP form.If an element is ‘*Not Applicable’*, you will be asked to enter a rationale for why the element does not apply to your organisation.In general, OVIC expects that the majority of Elements will be applicable and only a few may not be.N.B. If an element is managed by a third party, that does not mean that the element is not applicable to the organisation. As the risk owner, the organisation needs to have a level of oversight over elements that are managed by third parties, which should be reflected in your PDSP. |
| Much of our IT functions are outsourced to contracted service providers. Does this mean we can mark the IT Elements as not applicable? | No. Although you’ve contracted a service provider to undertake certain business functions on the organisation’s behalf, as the risk owner, you still need to maintain a level of oversight to ensure that specific risks to the business are being addressed by the provider.Where business functions are outsourced, organisations should ensure the intention of the element is being objectively met by the third party, and on-going assessments should also be made. |
| We don't currently use any control libraries. Are there any control libraries that are more closely aligned with the PDSP for small organisations? | The VPDSS Elements themselves can be considered a control library. If you intend to use the Elements in support of a particular program of work, please select ‘*VPDSSE’* in the ‘Control Library’ column in Part B of the PDSP. |
| Which business unit is responsible for managing the PDSP? | This very much depends on the organisation. Each business unit will be able to provide a unique insight into the information security arrangements of your organisation. Regardless of who manages the PDSP, OVIC encourages collaboration across all areas of the business to gain a better level of understanding and oversight in your PDSP. |
| Would you accept a hard copy PDSP submission? | Yes. While the preference is to receive your PDSP electronically, OVIC recognises this may not be possible in some instances. If you have any concerns about submitting your PDSP, please contact a member of the Information Security Unit by emailing security@ovic.vic.gov.au. |
| How can we reflect a continuous improvement process in the PDSP? Our program of work each year will strive to improve, so we rarely would see anything completed? | If there are projects or processes that you’re particularly proud of and have seen some improvement since the last reporting cycle we’d love to read these in the ‘*Security program executive summary from the past 24 months*’ section of your PDSP (pg. 9 of the PDSP form).The PDSP form also asks you to perform a maturity assessment for each Standard (outlining a current, target and aspirational maturity level), which offers another opportunity to highlight continuous improvement in organisational security practices. |
| How were the Elements derived? | The VPDSS Elements have been derived from a number of sources including ISO standards, Australian Standards, Victorian Government publications, and best practice guidance.For more information, please see the VPDSS implementation guide available from [OVIC’s website](https://ovic.vic.gov.au/data-protection/standards/). |
| The PDSP form has changed significantly since the first reporting period in 2018. What changes can we expect in future? | At OVIC, we are continually trying to improve the way we engage with organisations.The latest iteration of the PDSP is presented in PDF form, simplifying the way organisations can represent their security plans, and assisting OVIC in analysing statistics that fall out of this reporting period.  |
| Where can I find more information such as practitioner guides, factsheets, forms, and templates? | Visit the [VPDSF resources](https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/) page of the OVIC website. Additionally, if you’re an information security practitioner and would like to stay informed in relation to all things VPDSF you can join the [VISN](https://ovic.vic.gov.au/data-protection/for-agencies/victorian-information-security-network/).As a member of the VISN, you will receive correspondence of upcoming information security events and forums and can be added to the GovTEAMS online community where you will find additional content including draft publications, guidance material, and the opportunity for collaboration with network members.For more information about the VISN, please visit our [website](https://ovic.vic.gov.au/data-protection/for-agencies/victorian-information-security-network/). |
| Other |
| Should not-for-profit/ non-government organisations also should follow the VPDSF? | Generally speaking, not-for-profit/ non-government organisations are not bound by Part 4 of the PDP Act and are under no legislative obligation to follow the VPDSF. We do however recommend uptake of the VPDSF as a best practice model. Not-for-profit/ Non-government organisations who are providing a service or function on behalf of a Victorian government organisation, may be asked the ‘in-scope’ organisation to comply with the VPDSF for their own assurance purposes. This does not mean you must report to OVIC, you should seek clarification from the organisation about their assurance expectations.  |
| What is the biggest change we should be aware of with the new Framework (V2.0)? | The biggest changes to the VPDSF 2.0 is the refinement of the document to focus on assurance outcomes for OVIC, and organisations. Much of the language in the document has been simplified and certain chapters have been extracted and made into stand-alone documents. |
| Where can I find more information about best practice with regard to third party assurance? | OVIC is currently developing material on this topic.If you have any specific questions, please feel free to get in touch with the ISU by emailing security@ovic.vic.gov.au. |

Further Information

**Contact Us**

**t:** 1300 00 6842
**e:** enquiries@ovic.vic.gov.au
**w:** ovic.vic.gov.au**Disclaimer**

This fact sheet does not constitute legal advice and should not be used as a substitute for applying the provisions of the Freedom of Information Act 1982, or Privacy and Data Protection Act 2014 or any other legal requirement, to individual cases.