Office of the Victorian Information Commissioner

INFORMATION FOR AGENCIES

Information Security Incident Notification Scheme

What is the scheme?

The information security incident notification scheme has been developed to centrally coordinate notification of information security incidents (**incidents**) within Victorian government. It is established under Element E9.010 within the Victorian Protective Data Security Standards (**VPDSS**) that stating:

*The organisation notifies OVIC of incidents that have an adverse impact on the confidentiality, integrity, or availability of public sector information with a business impact level (**BIL**) of 2 (limited) or higher.*

Where information assets have been assessed as BIL 2 or higher, organisations are encouraged to notify OVIC *of any incidents* that compromise the confidentiality, integrity and/or availability (**CIA**) of that information.

If the information has not been assessed and/or assigned a BIL rating yet, but an incident occurs, you may contact OVIC to discuss.

For more information on how to assess the business impact level of an information asset, refer to VPDSF Practitioner Guide: Assessing the Security Value of Information.

Benefits of the scheme

The scheme benefits all who participate by providing tangible resources, trend analysis and risk reporting.

Notification of incidents affecting public sector information should not add unnecessarily to the incident management and response process for organisations.

What is an information security incident?

An information security incident is defined as:

one or multiple related and identified security events that can harm/damage an organisation, its assets, individuals or compromise its operations.
Information security incidents may take many forms, such as compromises of electronic information held on government systems and services and include information in physical formats e.g., printed, photographs, or recorded information either audio or video, and verbal discussions.

Information security incidents can include privacy breaches.

Privacy breach considerations

If an incident relates to a breach of personal information, consider the impact on individuals and the need to notify them in a timely manner. Although some impacts may not appear high to the business, they may be for individual(s).

For more information regarding incidents involving a privacy breach, refer to Managing the Privacy Impacts of a Data Breach on OVIC's website.

Who can notify OVIC when an incident occurs?

OVIC accepts notifications from anyone. The representative may be an information security lead (**ISL**), privacy officer, Chief Information or Security Officers (CIO, CISO), legal officer or public sector body Head.

For representatives submitting a notification on behalf of their organisation, please follow your incident management authorisation process to avoid duplicate submissions for the same incident.

Who do I turn to for assistance when an incident occurs?

Every incident has unique characteristics and may require different approaches for resolution. The table below provides guidance where agencies or bodies can seek assistance.

	Incident Management (who is …?)			
If an incident is due to….	**Responsible**	**Accountable**	**Consulted**	**Informed**
A lost document	Organisation	Organisation	Organisation	OVIC
Corrupt conduct of an individual	Organisation	Organisation	IBAC	OVIC
Physical access intrusion	Organisation	Organisation	Organisation	OVIC

	Incident Management (who is …?)			
If an incident is due to….	Responsible	Accountable	Consulted	Informed
Cyber intrusion	Organisation	Organisation	CIRS[1] *(if cyber response assistance is required)*	OVIC
Breach of personal information	Organisation	Organisation	Organisation	OVIC

How can I seek assistance in managing an urgent and significant incident?

OVIC does not provide an incident response service. If you require immediate assistance for cyber incidents, please contact the Cyber Incident Response Service (CIRS) directly on 1300 278 842.

What sort of incidents does OVIC accept?

Under element E9.010, VPS organisations are encouraged to notify OVIC of incidents that have an adverse impact on the confidentiality, integrity and/or availability of public sector information with a business impact level (BIL) of 2 (limited) or higher.

This includes information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET. Refer to your organisation's BIL table or the VPDSF BIL table to assess the potential business impact level of the information affected in the incident.

Incidents may take many forms. They are not just limited to compromises of electronic information held on government systems and services but also include compromises of information held in physical formats (e.g., printed, photographs, recorded information either audio or video) or unauthorised verbal discussions. For example, the following scenarios would qualify as an incident:

- leaving a sensitive hard copy document on public transport
- someone tailgating personnel into a secure area where sensitive documentation is kept, and/or
- a sensitive conversation being overheard in a public cafe by a member of the public.

Incidents may affect different types of public sector information. OVIC encourages organisations to notify us of incidents that affect all types of information for example financial, policy, operational, legal, and not just personal information.

If the incident is of a criminal nature or involves fraud/corruption, please follow your organisation's policy on reporting these types of incidents to the relevant bodies.

[1] Victorian Government Cyber Incident Response Service (**CIRS**). Refer to the CIRS website for more information https://www.vic.gov.au/victorian-government-cyber-incident-response-service

The table below provides further examples of the types of incidents that OVIC can accept under the ISINS.

Examples of incidents affecting public sector information	Control area	Security attribute
Sending an email to incorrect email recipient	People/ process	Confidentiality
Hard copy document/file left on public transport	People/ process	Confidentiality/ Availability
Tailgating into a secure area and accessing documents left on someone's desk	Process	Confidentiality
Ransomware installed on a desktop restricting access to information	Technology	Availability
Incorrect protective marking placed on a document leading to mishandling of information	People	Confidentiality
A break-in to a facility and stealing information	Process	Confidentiality/ Availability
A conversation being held in a public area that can be easily overheard	People	Confidentiality
Viewing information on an unlocked screen by someone who does not have a 'need-to-know'	Process	Confidentiality
Looking at documents left on a printer	People	Confidentiality
Incorrectly disposing of hard copy documents in recycling bin	People/ process	Confidentiality
Documents found in an unused cabinet/vacated premises	Process	Confidentiality
Information found on a decommissioned laptop/computer at a second-hand store	Process	Confidentiality
Information found on a lost unencrypted USB key	Process	Confidentiality/ Availability
Personnel undertaking unauthorised activity on systems e.g., manipulating/changing data on a database	People	Integrity
Disclosing classified information at a social gathering	People	Confidentiality

Examples of incidents affecting public sector information	Control area	Security attribute
Hacker exfiltrating sensitive information to an external system	People/ technology	Confidentiality
Outsider launching a denial-of-service attack on a website	People/ technology	Availability

Remember, your organisation's Business Impact Level (**BIL**) table may be used to inform notification of an incident to OVIC. If the information affected by the incident has a security value of BIL 2 (e.g., OFFICIAL: Sensitive) or higher assigned to it (regardless of the severity of the actual incident), notification should be considered.

For more information on how to conduct a security value assessment and determine the BIL value of the information affected in an incident please refer to *Practitioner Guide: Assessing the security value of public sector information*.

If public sector information does not have a BIL assigned, the business owner should be consulted to determine its security value including the potential impact of a compromise to the confidentiality, integrity and/or availability of the information.

When to notify OVIC

Organisations are encouraged to notify OVIC of an incident as soon as practical and no later than 30 days once an incident has been identified. If a response capability is required, organisations are encouraged to seek support from:

- their own internal security resources
- their parent entity (if one exists), and
- the Victorian Government's Cyber Incident Response Service (**CIRS**) in the event of a cyber incident.

How to notify OVIC of an information security incident

There are several methods to notify OVIC of an incident including:

Method	Options
Form	Fill in the incident notification form available on our website. Please provide as much detail as possible. **Option 1:** Online web form – • Access via https://incident-notifications.ovic.vic.gov.au/ • Once completed, please hit '*submit incident notification*' **Option 2:** Download a word version of the incident notification form -

Method	Options
	• Once completed, assess the content of the completed form and apply a corresponding protective marking (OFFICIAL, OFFICIAL: Sensitive or PROTECTED). • Submission options depend on the protective marking of the content contained in the incident notification form. For content marked: - OFFICIAL or OFFICIAL: Sensitive, please email a copy of the form as an attachment to incidents@ovic.vic.gov.au, or - PROTECTED or above, please contact a member of the Information Security Unit for advice on submission options.
Email	Send an email to incidents@ovic.vic.gov.au with the incident details.
Phone	Call 1300 00 OVIC (1300 006 842) to discuss the incident.

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.

Where you provide personal information, OVIC may use it to provide you with confirmation of receipt of your notification, seek clarification on the contents of your notification 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 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.

For further information on how OVIC handles personal information, please review our 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.

What happens after OVIC is notified of an incident?

OVIC will acknowledge receipt of the notification and provide a reference number in case of any follow up communication regarding the notification.

Where information about the incident is incomplete or not yet available, OVIC can receive updates from the notifying organisation as they become available.

OVIC may contact you in the following circumstances:

- if your notification did not provide enough detail about the incident, we may request more information from you
- if your notification points to a potentially serious or systemic breach of the *Privacy and Data Protection Act 2014* (Vic) (PDP Act), we may contact you to make enquiries in accordance with OVIC's Regulatory Action Policy

OVIC may use the information provided in incident notifications for the purposes of identifying trends, themes and risks published in our biannual reports for organisations to use, research projects or activities set out in OVIC's Regulatory Action Policy. To support these activities, information should be timely, accurate and complete.

How does OVIC use incident notifications?

Incident notifications assist OVIC to develop a comprehensive security risk profile of participating agencies and bodies. This can be used for trend analysis and understanding of the threat environment as it relates to the protection of public sector information.

OVIC may share de-identified data with partnering organisations.

OVIC publishes incident insights reports about trends and themes observed through the notifications. These reports are designed to assist organisations' own risk reporting forums, inform their own risk assessments and preparation of business cases for strategic security initiatives.