Office of the Victorian Information Commissioner

INFORMATION FOR
THE PUBLIC/AGENCIES

1300 00 6842 | ovic.vic.gov.au

Information security incident notification scheme

What you need to know

What is the scheme?

The information security incident notification scheme benefits all who participate and provides tangible resources, trends analysis and risk reporting. Notification about information security incidents (incidents) affecting public sector information should not add unnecessarily to the incident management and response process for organisations.

Element E9.010 within the Victorian Protective Data Security Standards (**VPDSS**) states:

*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.*

The information security incident notification scheme has been developed to centrally coordinate notification of information security incidents (**incidents**) within Victorian government. It requires Victorian public sector (**VPS**) agencies or bodies to notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information that have been security assessed as having a 'limited' business impact or higher[1] on government operations, organisations, or individuals.

Who can notify OVIC when an incident occurs?

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

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.

Information security incident as a result of ….	Incident Management (who is …?)			
	Responsible	Accountable	Consulted	Informed
A lost document	Organisation	Organisation	Organisation	OVIC

[1] Refer to the current VPDSF BIL table on the OVIC website https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/ for further information.

Corrupt conduct of an individual	Organisation	Organisation	IBAC	OVIC
Physical access intrusion	Organisation	Organisation	Organisation	OVIC
Cyber intrusion	Organisation	Organisation	CIRS[2] *(if response assistance is required)*	OVIC
Breach of personal information	Organisation	Organisation	Organisation and OVIC *(if privacy guidance is required)*	OVIC

What sort of incidents should I notify OVIC of?

Under element E9.010, VPS organisations are required to notify OVIC of any compromise of public sector information that may cause 'limited' (BIL 2) or higher harm/damage to government operations, organisations, or individuals. This includes information with a protective marking of OFFICIAL: Sensitive, PROTECTED, Cabinet-In-Confidence or SECRET.

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.

If the incident is of a criminal nature, please follow your organisation's policy on reporting these types of incidents to law enforcement authorities.

The table below provides further examples of the types of incidents that OVIC should be notified about.

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

[2] 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

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

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

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*[3].

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 should I notify OVIC?

Organisations should 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.

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).

OVIC can assist with responding to incidents related to personal information. Where assistance is required, contact OVIC's privacy team and refer to OVIC's website for supporting resources: https://ovic.vic.gov.au/privacy/managing-the-privacy-impacts-of-a-data-breach/

How do I notify OVIC of an incident?

OVIC has published an incident notification form[4] on its website for organisations to complete and submit. There are several methods to notify OVIC of an incident including:

- emailing your completed incident notification form to incidents@ovic.vic.gov.au; or
- phoning 1300 00 OVIC (1300 006 842).

Emailing your completed incident notification form is the preferred approach as it is the easiest method to ensure all submission details are accurately completed, recorded and, if requested, passed onto the relevant area e.g., OVIC's Privacy team or CIRS.

What information should I provide?

OVIC, organisations and Victorian government will use the information provided in incident notifications to inform critical business decisions. To support these decisions, information must be timely, accurate and complete.

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

OVIC has identified some key fields for organisations to consider when submitting their information

[3] Refer to the resources page on our website https://ovic.vic.gov.au/data-protection/information-security-resources/

[4] Refer to the resources page on our website for a copy of the form https://ovic.vic.gov.au/data-protection/information-security-resources/

security incident notification. The information security incident fields include:

Incident notification fields	Description
GENERAL DETAILS	
Name of organisation	
Contact details	Provide the primary point of contact details for OVIC to correspond with if further information is required including name, phone number, email address.
When did it happen?	DD/MM/YYYY
When did the organisation become aware of it?	DD/MM/YYYY The date the incident is discovered and recorded may differ from the date when it occurred.
What happened?	Summary of what happened and what are you doing about it? Free text field with a short description of the incident.
How did it happen?	For example: • Who / what caused it? • Was 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	
PRIVACY (PERSONAL INFORMATION) INCIDENTS	
What personal information is involved?	Provide details e.g., name, contact details, Information Privacy Principle (**IPP**) 10[5] categories of sensitive information.
What is the risk of harm to the affected individuals?	• What type of harm? • How serious is the risk of harm? • How likely is the risk of harm?

[5] Refer to IPP 10 explanation on our website https://ovic.vic.gov.au/book/ipp-10-sensitive-information/

Incident notification fields	Description
Have affected individuals been notified about the incident?	If not, why? If so, how? What were the reactions?
INCIDENT NOTIFICATION SCHEME	
What type of information was affected?	What information asset has been affected? For example, financial, personal, legal, health, policy, operational, critical infrastructure.
What is the assessed business impact level (BIL) of the affected information?	What is the highest business impact level of the affected information? Select the one that applies: • BIL 1 – Minor; • BIL 2 – Limited; • BIL 3 – Major; or • BIL 4 – Serious.
What security attributes were affected?	Select all that apply: • Confidentiality (unauthorised disclosure); • Integrity (unauthorised modification); and/or • Availability (lost, stolen, unavailable).
What was the format of the affected information?	Select one that applies: • Hard copy; • Electronic; and/or • Verbal.
Was the incident primarily caused by people, process and/or technology control(s)?	Select any that apply: • People; • Process; • Technology; and/or • No control(s) in place.
Who caused the incident?	Select the one that applies: • Internal personnel; • Authorised third party; • Other external; or • Other/ unknown.

Incident notification fields	Description
What was the threat type?	Select one that applies: • Accidental / Error; • Failure; • Malicious; or • Natural.
For cyber incidents, is incident response assistance required by the Cyber Incident Response Service (CIRS)?	Y/N If you require incident response assistance and would like OVIC to send these incident details to CIRS on your behalf, please select **Y**. Please note: OVIC do not provide a 24/7 service so if you require immediate assistance, please contact CIRS directly on 1300 278 842.
For incidents relating to personal information, is privacy assistance required by OVIC?	Y/N If you require privacy assistance, please select Y and someone from the OVIC privacy team will contact you.
Has this incident been recorded in your organisation's incident register?	Y/N If Y please provide incident reference.
Has the incident been closed?	Y/N

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.

In most cases, there will be nothing further required.

However, 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; or
- if your notification indicates a risk of harm to the people whose personal information was involved, we may contact you to provide guidance about managing the privacy impacts of the data breach.

How does OVIC use incident notifications?

Incident notifications assist OVIC to develop a comprehensive security risk profile of the Victorian government. 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 and may also share outcomes of its incident analysis with the Cyber Incident Response Service (**CIRS**).

OVIC publishes regular incident insights reports[6] about trends and themes observed through the notifications. These reports are designed to assist organisations own risk reporting forums, and preparation of business cases for strategic security initiatives.

Further Information

Contact Us

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

[6] Refer to the resources page on our website for our incident insights reports https://ovic.vic.gov.au/data-protection/information-security-resources/