Office of the Victorian Information Commissioner

INFORMATION FOR
AGENCIES and BODIES

1300 00 6842 | ovic.vic.gov.au

Information security incident notification scheme

Things you need to know

The incident notification scheme will benefit all who participate and provide tangible resources, trends analysis and risk reporting. Notification about incidents affecting public sector information should not add unnecessarily to the incident management and response process.

OVIC will, on a regular basis, provide assistance to all engaged entities by reporting on the current trends using information from verified sources such as the national Cyber Security Operations Centre (CSOC), Open Source Intelligence (OSINT) and industry verified resources. Analysis of notified incidents by OVIC will also be documented. These reports will be provided on a quarterly basis and should assist with organisations own risk reporting forums and preparation of business cases for strategic security initiatives.

What is the scheme about?

Element E9.010 within the 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 scheme has been developed to centrally coordinate notification of information security incidents within Victorian government. It requires agencies or bodies to notify OVIC of incidents that compromise the confidentiality, integrity or availability of public sector information with a 'limited' business impact or higher[1] on government operations, organisations or individuals.

Incident notification assists OVIC with developing a comprehensive security risk profile of the Victorian government which can be used for trend analysis and understanding of the threat environment. OVIC will share de-identified outcomes of the analysis with Victorian Government agencies and bodies which will in turn inform their own risk assessments.

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 may for example be your security lead, privacy officer, CIO, CISO or public sector body Head.

[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.

Who to turn to for assistance when an incident occurs?

Every security incident has unique characteristics and may require different approaches to resolution. The table below provides some 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
Corrupt conduct of an individual	Organisation	Organisation	IBAC	OVIC
Physical access intrusion	Organisation	Organisation	Organisation	OVIC
Cyber intrusion	Organisation	Organisation	CIRS *(if response assistance is required)*	OVIC
Breach of personal information	Organisation	Organisation	Organisation and OVIC if guidance required	OVIC

What sort of information security incidents should I notify OVIC on?

Information security incidents may take many forms, they are not limited to compromises of electronic information held on government systems and services and also include information in physical formats (i.e. printed, photographs, recorded information either audio or video) and verbal discussions. For instance, leaving a sensitive hard copy document on public transport, someone tailgating into a secure area that has sensitive documentation available, a sensitive conversation being overheard in a public cafe.

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, for any compromise of public sector information that may cause 'limited' (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.

Examples of security incidents of sensitive information	Security area	Security attribute
Hard copy document/file left on public transport	Physical	Confidentiality/ Availability
Tailgating into a secure area and accessing documents left on someone's desk	Physical	Confidentiality

Examples of security incidents of sensitive information	Security area	Security attribute
Ransomware installed on a desktop restricting access to information	ICT/Cyber	Availability
Incorrect protective marking placed on document leading to mishandling of information	Information	Confidentiality
A break-in to a facility and stealing information	Physical	Confidentiality/ Availability
A conversation being held in a public area that can be easily overheard	Personnel	Confidentiality
Viewing information on an unlocked screen by someone who does not have a 'need-to-know'	Physical	Confidentiality
Looking at documents left on a printer	Physical	Confidentiality
Sending an email to incorrect email recipient	ICT/Cyber	Confidentiality
Incorrectly disposing of hard copy documents in recycling bin	Physical	Confidentiality
Documents found in an unused cabinet/vacated premises	Physical	Confidentiality
Information found on a decommissioned laptop/computer at a second-hand store	ICT/Cyber	Confidentiality
Information found on a lost unencrypted USB key	ICT/Cyber	Confidentiality/ Availability
Personnel undertaking unauthorised activity on systems e.g. manipulating/changing data on a database	ICT/Cyber	Integrity
Disclosing classified information at a social gathering	Personnel	Confidentiality
Hacker exfiltrating sensitive information to an external system	ICT/Cyber	Confidentiality
Outsider launching a denial of service attack on a website	ICT/Cyber	Availability

Remember the organisation's Business Impact Level (BIL) table should be used as a guide to inform your notification obligations in relation to an information security incident.

BIL's and how to conduct a security value assessment are determined by the business owner of the information and are explained further in our *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 the value of the information i.e. the 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 information security 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 Cyber Incident Response Service (CIRS) in the event of a cyber incident.

Privacy breach considerations

In the event, the 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 provide assistance regarding responding to incidents related to personal information. Where assistance is required, contact the OVIC privacy team and refer to the OVIC website for supporting resources https://ovic.vic.gov.au/privacy/for-agencies/responding-to-data-breaches/

How do I notify OVIC of an information security incident?

OVIC has developed an incident notification form that is available on the OVIC website for organisations to complete and submit. There are several methods to notify OVIC of an incident, these include:

- Email your completed incident notification form to incidents@ovic.vic.gov.au; or
- Phone 1300 00 OVIC.

Emailing your completed incident notification form is our 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 Privacy team or CIRS.

What sort of 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.

OVIC has identified some key fields for organisations to consider when submitting their information security incident notification.

Where information is incomplete or not yet available, OVIC can receive updates as they become available.

The information security incident fields include:

Incident notification fields	Description
Name of organisation	
Contact details	Provide the primary point of contact details for OVIC to correspond with where further information is required including name, phone number, email address.
Date incident occurred	DD/MM/YYYY
Date incident identified	DD/MM/YYYY The date the incident is discovered and recorded may differ from the date when it occurred
Incident summary	What happened and what are you doing about it? Free text field with a short description of the incident.
Information affected	What information asset has been affected? For example, financial, personal, legal, health, policy, operational, critical infrastructure)
Highest business impact level (BIL) of the affected information	What is the highest business impact level of the affected information? Select the one that applies: • 1 Minor • 2 Limited • 3 Major • 4 Serious
Business impacts as a result of the incident	What are the business impacts as a result of the incident? Select all that apply: • Economy and finance; • Legal and regulatory; • Personal; • Public services; and/or • Public order, public safety, law enforcement.
Incident type (security attribute affected)	What security attribute was affected? Select all that apply: • Confidentiality (unauthorised disclosure); • Integrity (unauthorised modification); and/or • Availability (lost, stolen, unavailable)

Incident notification fields	Description
Information format	What format was the information. Select all that apply: • Hard copy; • Electronic; and/or • Verbal.
Security area	Select all that apply: • Information • Personnel • ICT/Cyber • Physical
Proposed actions	Recommended actions to prevent future reoccurrence of the incident Free text field
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

Further Information

Contact Us

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