Read this before proceeding

|  |
| --- |
| How to use this optional guidance template |
| Remove all **blue** and **red** guidance text in this template as you build your plan.  This guidance template is prepared by the Cyber Security, Data and Digital Resilience Division in the Victorian Government Department of Government Services.  This is not a mandated format for your Cyber Security Incident Response Plan (CSIRP). It is one possibility of many.  You are the author of your plan. Your plan will be the result of your planning process. Using this guidance template does not guarantee that your plan is a high quality.  Your plan should be branded to align with your internal branding standards, as it is an internal document.  This template includes roles and responsibilities from:   * Victoria’s [Cyber Security Incident Management Plan](https://www.vic.gov.au/cyber-incident-management-plan) (October 2024) * [State Emergency Management Plan Cyber Security Sub-Plan](https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-sub-plans/state-emergency-management-plan-cyber-security-sub-plan-edition-2) (March 2024).   This guidance is prepared with reference to [ACSC’s cyber security incident response planning practitioner guidance](https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/incident-response/cyber-security-incident-response-planning-practitioner-guidance) (April 2024).  The template also includes a number of ‘good ideas’ to consider.  It is your responsibility to know what responsibilities are relevant to your department or agency. Your sector may have additional requirements for you to consider.  Your plan should be a plan for your whole department or agency. It is not only a plan for your cyber security team only. It will include responsibilities for other teams too.  You are encouraged to talk through each section of your plan with relevant stakeholders. This will help you agree on specific arrangements. Write those arrangements in this plan. This template is a prompt for these conversations.  This guidance template is generic. It is not prepared for your specific context. You should tailor this template to match your unique operating environment, priorities, existing resources and obligations. There is no limit to how much you may modify the template.  It is recommended that you hyperlink to pre-existing documents instead of duplicating it in this plan.  Your plan should be supplemented with detailed day-to-day processes, procedures, playbooks to aid response to common incident types and Standard Operating Procedures (SOPs) to incidents affecting specific assets. |

Cover page template

An optional guidance template for:

[department or agency name]

**Cyber Security Incident Response Plan**

for all severities of cyber security compromise

Version [date]

Template version 2: published May 2025

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| In the event of an incident:   * Use the **Incident Response Quick Reference Guide** on the next page (once guidance text is removed) * An Incident Action Plan template is at **Appendix X** * **Contact** the following: | | | | |
|  | Name | Role | Availability | Contact Details |
| Primary contact |  |  | e.g. 0700–1900 | Phone &  Email |
| Secondary contact |  |  | e.g. 0700–1900 | Phone &  Email |
| DGS’ Cyber Incident Response Service | | | 24/7 | [Victorian Government Cyber Security Portal](https://vicgov.sharepoint.com/sites/VG002650/SitePages/Incident-Reporting.aspx)  If outside business hours: 1300 278 842 |

## Incident Response Quick Reference Guide

While loosely sequential, many of these actions will need to occur concurrently. This is a quick reference guide only and is not a complete summary of the actions outlined in this plan.

|  |  |  |  |
| --- | --- | --- | --- |
| Action | Relevant section of this plan | Page | Summary of Activity |
| 1 | Analysis | X | Conduct initial analysis to determine whether an incident has occurred or is occurring |
| 2 | Classification | X | Determine the scope, impact and severity of the incident; categorise the incident |
| 3 | Notification | X | Make the required notifications |
| 4 | Management teams | X | Activate your Incident Management Team (and Senior Executive Management Team, if appropriate) to manage the response effort |
| 5 | All response sections | X | Prepare and then deliver the actions outlined in the Incident Action Plan |
| 6 | Closing out an incident | X | Stand down your Incident Management Team / Senior Executive Management Team (when authorised by appropriate delegate); determine any stakeholder communications requirements |
| 7 | Lessons and evaluation | X | Conduct a post incident review to identify things that worked well and any opportunities for improvement; document your learnings/insights |
| 8 | Preparedness | X | Update this Incident Response Plan to include any key learnings/insights, in preparation for the next incident. |

Publication information

[Who] approved this Cyber Security Incident Response Plan (CSIRP, or ‘the Plan’) on [date].

The Plan is prepared by [author/team].

The following teams provided input throughout the review process:

* the cyber security team
* I.T. team
* business continuity team
* risk team
* communications team
* emergency management team
* compliance and legal team

This document is available at [file path]. Physical copies of this plan, for access if internal systems are compromised, are available at [physical location/s].

Review

This Plan will be reviewed [insert frequency, e.g. 6 monthly or annually] or following any cyber security incident or significant change where a review is warranted.

This version of the plan has been updated with consideration to learning from previous incidents and exercises.

The next scheduled review is to be completed by [date] by [team/person managing the plan].

Plan activation

This plan is current at the time of its approval. It remains in effect until it is modified, superseded or withdrawn.

The arrangements in this plan are ongoing and do not require activation.

When a Whole of Victorian Government response to a compromise is required, this Plan will be enacted alongside either:

* the [**Victorian State Emergency Management Plan Cyber Security Sub-Pla**](https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-sub-plans/state-emergency-management-plan-cyber-security-sub-plan-edition-2)**n**, which addresses WoVG arrangements for cyber security emergencies.
* the [**Victorian Cyber Security Incident Management Plan (**](https://www.vic.gov.au/cyber-incident-management-plan)**CSIMP)**, which covers the 3 types of non-emergency incidents which need a WoVG response (limited, major and critical cyber security incidents).

Where there is unintentional conflict of this CSIRP with the Sub-Plan and CSIMP, the Sub-Plan and CSIMP take precedence.

Table of Contents

[Incident Response Quick Reference Guide 4](#_Toc198717989)

[1 Summary of this plan 8](#_Toc198717990)

[1.1 Overview 8](#_Toc198717991)

[1.2 Structure of this plan 8](#_Toc198717992)

[1.3 Audience 10](#_Toc198717993)

[2 Mitigation 12](#_Toc198717994)

[3 Preparedness (identify, protect and detect) 14](#_Toc198717995)

[3.1 Threat intelligence 14](#_Toc198717996)

[3.2 Identify and protect from cyber security risk 16](#_Toc198717997)

[3.3 Maintain and exercise plans and arrangements 17](#_Toc198717998)

[3.4 Detection 18](#_Toc198717999)

[4 Response 19](#_Toc198718000)

[4.1 Analysis 19](#_Toc198718001)

[4.1 Notification and classification 23](#_Toc198718002)

[4.2 Technical response, including containment and eradication 27](#_Toc198718003)

[4.3 Control and coordination 28](#_Toc198718004)

[4.4 Consequence management 28](#_Toc198718005)

[4.5 Relief (assistance to meet essential needs) 30](#_Toc198718006)

[4.6 Management Teams 30](#_Toc198718007)

[4.7 Operations room 33](#_Toc198718008)

[4.8 Internal communication 33](#_Toc198718009)

[4.9 Media and public communication 34](#_Toc198718010)

[4.10 Participating in a WoVG response 35](#_Toc198718011)

[5 Recovery 36](#_Toc198718012)

[5.1 Recovery 36](#_Toc198718013)

[5.2 Closing out an incident 37](#_Toc198718014)

[5.3 Lessons and evaluation 37](#_Toc198718015)

[6 Appendices 38](#_Toc198718016)

# Summary of this plan

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

## Overview

Victorian public sector organisations, including ours, are responsible for our own internal response to all cyber security events, incidents and emergencies (collectively referred to as ‘compromises’ throughout this plan). This internal response includes:

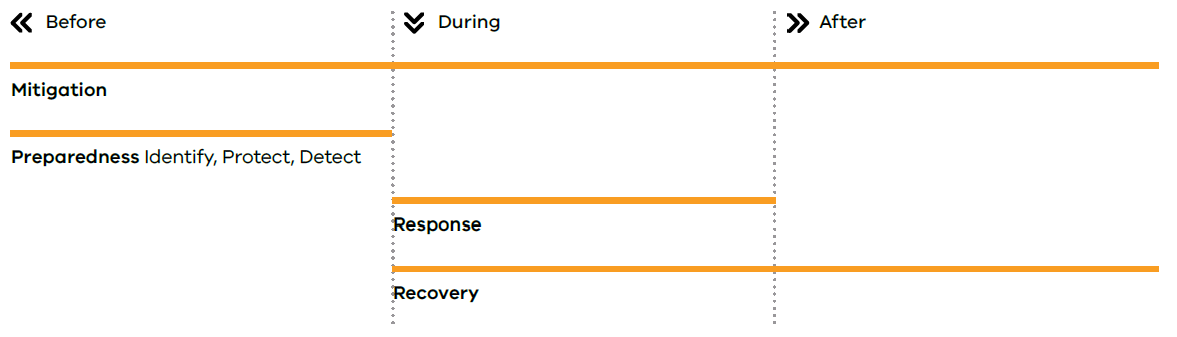
* technical cyber security response
* incident and emergency management arrangements
* consequence response
* communications.

Accordingly, this plan aligns with our responsibilities under the:

* State Emergency Management Plan Cyber Security Sub-Plan
* Victorian Cyber Security Incident Management Plan
* Victorian Protective Data Security Framework/Standards0F[[1]](#footnote-2)
* [sector specific frameworks and applicable regulations]
* Best practice.  
    
  Note: it is your responsibility to ensure that your CSIRP aligns with your responsibilities under these plans, frameworks etc.

## Structure of this plan

The format of this Plan aligns with the format of the State Emergency Management Plan Cyber Security Sub Plan, and the Victorian Cyber Security Incident Management Plan.

This Plan contains internal arrangements, roles and responsibilities for the mitigation of, response to and recovery from all severities of compromise.

1. **Mitigation**:actions at any point which stop or reduce the impact of incidents
2. **Preparedness (identify, protect and detect):** actions taken before a compromise, to be ready for it and its potential impacts.
3. **Response:** actions taken during a compromise to address it and its impacts.
4. **Recovery:** actions which address impacts after it has occurred.

## Audience

Internal use

This plan is primarily written for internal use. This includes, but is not limited to our:

* Impacted business area
* cyber security team
* I.T. team
* business continuity team
* risk team
* communications team
* emergency management team
* senior responsible executives.

Contracted and managed service providers

Additionally, we outsource to contracted service providers. We remain accountable for the outsourced service.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Service Provider | Service/s provided | Contact | Contact details | Service SLA |
| Name | Email management | Name, position |  | 8:00am to 5:00pm |
|  |  |  |  |  |
|  |  |  |  |  |

We ensure our contracted service providers do not contravene a protective data security standard in respect of public sector data collected, held, used, managed, disclosed or transferred by the contracted service provider.1F[[2]](#footnote-3)

We ensure that cyber security risk is managed in line with the risk and the value of the information or service. We achieve this through:

* [mechanism, e.g. contractual clause to ensure the implementation of what appropriate maturity model and framework]

Victorian Government

The Department of Government Services as Victoria’s lead portfolio department for cyber security, or [Department name] as the relevant sector portfolio Department for our entity, may request visibility of this Plan.

# Mitigation

Mitigation is not traditionally a component of an incident response plans; however, it is included for completeness, so that this one plan records actions relating to the full cyber security incident and emergency lifecycle.

|  |
| --- |
| Remove any content below which is not relevant.  If your entity has an existing written record of your cyber security maturity approach provide a link to it here instead of duplicating content. For example: link to the Protective Data Security Plan all VPS organisations are required to provide to OVIC under the Privacy and Data Protection Act 2014 (Vic).  If there is additional detail to add, consider including it as an appendix so it doesn’t detract from the response focus of this plan. |

.

* **ACSC’s Essential Eight Maturity Model (E8)**2F**[[3]](#footnote-4) and/or National Institute of Standards and Technology (USA) Cyber Security Framework (NIST)** 
  + [Detail which elements of have been applied AND which team/role is accountable]
* **Victorian Protective Data Security Framework & Standards**
  + [If applicable to your entity under the *Privacy and Data Protection Act 2014*, detail which elements have been adopted AND which team/role is accountable]
* **Information Security Manual** 
  + [Relevant if holding and accessing Commonwealth Government sensitive and security classified information AND which team/role is accountable]]
* ***Security of Critical Infrastructure Act 2018* (Cth)** 
  + [Relevant if required under this Act AND which team/role is accountable]]
* **Victorian Government Risk Management Framework (VGRMF)**
  + [If applicable to your entity, detail which elements have been adopted AND which team/role is accountable]
* **Australian Energy Sector Cyber Security Framework** 
  + [Relevant for the energy sector AND which team/role is accountable]
* ***Health Records Act 2001* (Vic)**
  + [Relevant if necessary to protect the privacy of individuals’ health information AND which team/role is accountable]
* **Other relevant standards**
  + [If necessary, detail other standards and their elements have been adopted AND which team/role is accountable]

# Preparedness (identify, protect and detect)

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

## Threat intelligence

Reviewing threat intelligence

[Person or team] is responsible to monitor threat intelligence, which is provided to [email address/es], and monitored [insert frequency, e.g. work hours only or 24/7/365].

|  |
| --- |
| If there is not 24/7/365 coverage, is it an untenable risk, and if so, how are these gaps addressed?  Contact [cybersecurity@dpc.vic.gov.au](mailto:cybersecurity@dpc.vic.gov.au) to request additional email addresses on the threat intelligence distribution lists. |

[Person or team] is responsible to review threat intelligence received to assess, detect potential exposure.

[Person or team] is responsible to implement mitigations as required.

Share threat intelligence

[Person or team] is responsible to report confirmed detections, information and intelligence to the Department of Government Services by email [cybersecurity@dpc.vic.gov.au](mailto:cybersecurity@dpc.vic.gov.au) or phone 1300 278 842.

[Person or team] will forward threat intelligence to the following people or teams, who will in turn decide if the intelligence is relevant and suitable under the given Traffic Light Protocol to share with the additional stakeholders.

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

## Identify and protect from cyber security risk

Managing information security risks

[Person or team] is responsible to follow the five steps in [OVIC’s action plan](https://ovic.vic.gov.au/resource/the-five-step-action-plan/)

1. identify information assets
2. determine the ‘value’ of this information
3. identify any risks to this information
4. apply security measures to protect the information
5. manage risks across the information lifecycle.

Policies, processes, playbooks and resources

[Person or team] is responsible to establish and regularly train/retrain users on cyber security policies listed in Appendix X

[Person or team] is responsible to develop and regularly train/retrain users on the playbooks at Appendix X, which consider disaster recovery and initial actions required.

[Person or team] is responsible to create incident response processes and procedures listed in Appendix X, using this plan as a basis.

[Person or team] is responsible to document critical processes, asset details, network topographies and key contacts (See **Appendix X**)

[Person or team] is responsible to maintain an up-to-date list of hardware and software, including cloud-based applications and virtual infrastructure (See **Appendix X**).

[Person or team] is responsible to update resources to ensure access to the latest:

* network diagrams
* IP addressing schemas
* port lists
* system logs
* system designs/architecture, security plans and GPO configuration.

Business Continuity Plans

[Person or team] is responsible to develop and regularly train/retrain users on a Business Continuity Plan [BCP link], in case critical assets need to be taken offline, with consideration to disaster recovery and initial actions required (e.g. first 72 hours). (See **Appendix X**)

Cyber insurance

[Person or team] is responsible to review cyber insurance arrangements at least annually.

Currently, we are insured for [summary of policy] by [insurance company].

## Maintain and exercise plans and arrangements

[Person or team] is responsible to conduct an annual exercise of this plan.

[Person or team] is responsible to ensure any areas for improvement identified in exercises are considered at the point that this plan is next updated.

|  |
| --- |
| An exercise may be as simple as an internal discussion, or as a detailed multi-agency deployment-style exercise.  The Australian Institute for Disaster Resilience’s [Managing Exercises Handbook](https://knowledge.aidr.org.au/resources/handbook-managing-exercises/) is an invaluable resource for how to exercise, from start to finish.  The ACSC has also prepared ‘[Exercise in a Box](https://exerciseinabox.cyber.gov.au)‘ scenario resources.  Exercises may include cyber and emergency management personnel, multi-agency stakeholders (such as critical infrastructure) or relevant community members and groups.  Requests for the Department of Government Services’ to be involved in the concept, design and/or delivery in your exercise can be provided to [cybersecurity@dpc.vic.gov.au](mailto:cybersecurity@dpc.vic.gov.au). The Department of Government Services is unable to provide direct support to all cyber security exercises and will prioritise providing support to entities carrying the highest risk for Victorians (e.g. critical infrastructure), if resourcing allows. |

[Person or team] is responsible to educate [management roles or groups] about the roles of executive and senior management in this plan.

[Person or team] is responsible to assess gaps in internal capability and capacity for this plan’s roles and responsibilities, processes and procedures. This assessment will be conducted [frequency] and [person or team] is accountable to address identified gaps.

|  |
| --- |
| For example, if maintaining sustainable staffing of an incident response is an identified gap, it may require:   * engaging a contracted service provider to supplement internal capability and capacity, and/or * engaging an insurance provider to see what additional resources are available. |

## Detection

[Person or team] is responsible to continuously monitor assets to find anomalies, indicators of compromise and other potentially adverse events.

[Person or team] is responsible to ensure appropriate logging and monitoring capability is in place to detect, understand and analyse event logs and identify incidents.

[Person or team] is responsible to liaise with the following Managed Service Providers to ensure threats are detected, analysed, communicated and managed consistent with the intent of this plan, where a Managed Service Provider is used to provide threat detection and analysis services.

[Person or team] is responsible to review log entries and security alerts to determine if there are any unusual entries or signs of suspicious behaviour on the network or applications.

[Person or team] is responsible to develop standard operating procedures for different operating systems on what to look for or review (such as, specific event log sources, the types of events to search for).

[Person or team] is responsible to consult with network and application experts to determine if there is a legitimate explanation for unusual or suspicious activity.

[Person or team] is responsible to research and review any open-source materials (including via internet search engines) relating to unusual or suspicious activity. For example, perform a search on any unusual filenames on the network.

[Person or team] is responsible to develop a watch list/monitor list of suspected accounts or IPs to monitor their ongoing activity.

[Person or team] is responsible to conduct investigations securely through a contracted service provider3F[[4]](#footnote-5).

# Response

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

## Analysis

[Person or team] is responsible to undertake initial analysis to determine scope, impact and severity of a cyber security compromise (in line with **Table 1**). Incident notifications must then commence in line with the ‘Notification and classification’ section below, noting the stipulated time parameters for certain notifications.

[Person or team] is then responsible to undertake further analysis, while incident notifications and other response activities are being completed. This includes:

* assess the BIL (see Appendix X)
* collect and record evidence to support forensic investigations. if necessary, seek advice from [digital forensic professional], [legal advisors] or [law enforcement].
* collate and securely store all collected evidence
* maintain a log of all evidence collected, using the template at Attachment X.

|  |
| --- |
| Evidence may include:  hard drive images, raw images and RAM images   * IP addresses * network packet captures and flows * network diagrams * log and configuration files4F[[5]](#footnote-6) * databases * incident response and investigation notes * screenshots * social media posts * CCTV, video and audio recordings * documents detailing monetary cost of remediation or loss of business activity |

|  |  |  |  |
| --- | --- | --- | --- |
| These are the categories used at a WoVG level. Note that the WoVG categories are focused at a state-scale, not at entity-scale. | | | |
| Severity (low to high) | WoVG category | Common traits of the WoVG category  These categories are prepared as a comparable state-level equivalent to the Office of the Victorian Information Commissioner’s (OVIC’s) entity-level Business Impact Levels (BILs). BIL’s are entity-specific and cannot be equated to a state level. | Entity specific detail that could result in the WoVG category or an entity-specific equivalent. |
| 1 | Event | A cyber security compromise that causes no impact to systems, services or information (such as, malicious scanning activity). | For example:   * BIL# * Spam email with no embedded URL’s or attachments * Automated malware detection alert requiring no further action. Single device, infection cleaned * General cyber security advice * False positive security alerts. |
| 2 | Minor | This is a successful cyber security compromise. The compromise has potential to cause or is causing minor impact to services, information, assets, reputation or relationships.  This involves:   * a response using routine internal procedures, within our normal response capability and capacity * an assumption that the incident will not spread to another department or government agency. | For example:   * BIL# * <10% of non-critical staff affected temporarily (short term) * Minimal, if any, impact * One or two non-sensitive/non-critical machines affected * No breach of data * Negligible risk to reputation. |
| 3 | Limited | This is a successful cyber security compromise. The compromise has potential to cause or is causing limited impact to services, information, assets, government reputation, relationships and/or the community.  This involves at least one of the following consequences:   * direct or indirect impacts to our ability to ensure the confidentiality, integrity or availability of its systems, services or data * disruption to activities requiring reprioritisation of activities or resourcing to meet expected levels of service * impacts to critical business operations and other systems * potential to spread to another department or government agency * a response required at the state level, involving:   + monitoring and analysis   + sharing indicators of compromise, mitigation advice and options * a need to coordinate a WoVG response in support of a Commonwealth-led incident.   Alternatively, it can mean a cyber security threat where there is:   * a major scheduled event which may be an attractive target for a cyber attack * information or intelligence that identifies a cyber security threat that warrants increased monitoring and analysis. | For example:   * BIL# * 20% of staff unable to work * Small number of non-critical systems affected * Possible breach of small amounts of non-sensitive data * Financial impact greater than $25,000 * Low risk to reputation. |
| 4 | Major | This is a successful cyber security compromise. This compromise has potential to cause or is causing major impact to services, information, assets, government reputation, relationships and/or the community.  This involves at least one of the following consequences:   * ineffectiveness of our ability to ensure the confidentiality, integrity or availability of systems, services or data * disruption to activities requiring reprioritisation of activities or resourcing to meet expected levels of service * activation of business continuity plans * direct or indirect major impacts to more than one department or government agency * a large-scale data breach * media interest generated by public concern * an immediate response required at the state level, involving strategic coordination and engagement to:   + advise stakeholders, detailing the threat and potential or actual impacts   + share indicators of compromise, mitigation advice and options * develop and/or share response capability across jurisdictions * engage media, government and Victorians * consideration to share and deploy technical resources across departments and request Australian Cyber Security Centre (ACSC) assistance * a need to coordinate a WoVG response in support of a Commonwealth-led incident or crisis.   Alternatively, this can mean a cyber security threat where information or intelligence warrants immediate monitoring and analysis (e.g. increased cyber threat activity, which may extend across Victoria or nationally). | For example:   * 50% of staff unable to work * Non-critical systems affected * Risk of breach of personal or sensitive data * Financial impact greater than $50,000 * Potential serious reputational damage. |
| 5 | Critical | This is a successful cyber security compromise. This compromise has potential to cause or is causing significant impact to services, sensitive information, assets, government reputation, relationships and/or the community.  This involves at least one of the following consequences:   * sustained disruption to our ability to ensure the confidentiality, integrity or availability of its systems, services or data, directly or indirectly * malicious cyber activity where the cause and potential extent is uncertain * links across multiple departments, government agencies or Australian jurisdictions requiring a coordinated WoVG response * an immediate response required at the state level, involving strategic coordination and engagement to:   + advise stakeholders, detailing the threat and potential or actual impacts   + share indicators of compromise, mitigation advice and options * develop and/or share response capability across jurisdictions * engage media, government and Victorians * consider sharing and deploying technical resources across departments and government agencies, and request Commonwealth assistance. | For example:   * Over 80% of staff (or several critical staff/teams) unable to work * Critical systems offline * High risk to/definite breach of sensitive client or personal data * Financial impact greater than $100,000 * Severe reputational damage – likely to impact business long term. |
| 6 | Emergency | This is a serious or exceptional compromise of cyber security. This compromise has potential to cause or is causing at least one of the following consequences:   * death or serious injury * extensive damage to property, infrastructure or the environment * widespread disruption, damage or destruction of critical infrastructure * disruption to emergency services requiring reprioritisation to meet expected levels of service * significant adverse consequences for some or all Victorians * large-scale economic consequences to Victoria. | For example:   * A death or serious injury attributable to a consequence of the incident |

## Notification and classification

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

Internal notifications

[Person or team] is responsible for making the following internal notifications.

|  |
| --- |
| Consider which notifications should be made following consultation with your legal/security/regulatory team. Ensure those details are captured here.  Are there internal notifications that are missing that should be represented here?  Consider what severity of incident will trigger what notifications, and document it here. |

External notifications

[Person or team] is responsible for the external notifications in this section.

|  |
| --- |
| Ensure that these notifications align with what is required under the CSIMP and Sub-Plan.  The example included here is tailored to an agency, not a department. For example, the CSIMP/Sub-Plan includes other stakeholders, e.g. a Minister’s Office. |

## Technical response, including containment and eradication

[Person or team] is responsible to lead our technical response.

[Person or team] is responsible to develop and implement an internal incident response plan which details containment, eradication and recovery activities.

[Person or team] is responsible to seek assistance from DGS’ Cyber Incident Response Service if more technical resources are needed.

[Person or team] is responsible to undertake containment actions, considering:

* any additional impacts there could be to systems, services or networks
* time and resources required to contain the cyber security incident
* effectiveness of the containment solution (e.g. partial vs full containment)
* duration that the containment solution will remain in place (e.g. temporary vs permanent solution).

|  |  |  |
| --- | --- | --- |
| Type | Description | Initial response to minimise potential harm |
| Ransomware | A tool used to encrypt or lock victims’ data until a ransom is paid. | Immediately remove the infected device/s from the network to limit the spread of ransomware.  Capture all available logs relevant to the device.  Isolate the devices while containment and eradication activities are determined. |
| Malware infections | A code-based malicious entity that successfully infects a host (such as virus, worm or trojan horse). |
| Denial of Service (DoS) /Distributed Denial of Service (DDoS) attacks | Overwhelming a network with traffic that it cannot process, sometimes causing the network to fail. | Request gateway services provider to identify DoS/DDoS nature, attack vector and implement suitable solutions.  Liaise with gateway services and network team to apply filters at network edge and/or increase capacity. |
| Phishing and social engineering | Deceptive communication designed to elicit users’ sensitive information (including network credentials). | Review logs of affected users (web and email logs) to determine whether malicious links/attachments were accessed.  Consult users to confirm what actions they took and whether any personal/sensitive information was provided in response to a phishing/social engineering attempt.  Consider resetting user passwords  Monitor accounts for any unauthorised access. |
| Data breach | Unauthorised access to sensitive or personally identifiable information (including public sector data). | Contain the data loss/spill as soon as possible.  Alert privacy, legal and communication/media teams  Investigate the cause of the data loss/spill.  For more information, refer to the OVICs [Managing the Privacy Impacts of a Data Breach](https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/). |

## Control and coordination

[Person or team] is responsible to seek assistance from DGS’ Cyber Incident Response Service if more non-technical resources are needed (e.g. communications support).

[Person or team] is responsible to appoint an Incident Manager and advise DGS’ Cyber Incident Response Service.

[Person or team] is responsible to maintain a written record of decisions made throughout the duration of the incident (See **Appendix X**)

[Person or team] is responsible to follow, where useful, the incident management guidelines set out in the Australasian Inter-Service Incident Management System (AIIMS) (See **Appendix X**). This may include creating an internal incident management team to delegate roles to (see the Incident Management Team section).

## Consequence management

Portfolio [insert portfolio responsibility here]

[Person or team] is responsible manage its own response to any consequence impacting the portfolio.

[Person or team] is responsible to liaise with relevant stakeholders.

[Person or team] is responsible to create and enact an action plan to address the consequences for areas of portfolio responsibility.

[Person or team] is responsible to activate business continuity plans as needed.

[Person or team] is responsible contact insurance provider for guidance (e.g. on evidence collection, relief activities and level of support required).

[Person or team] is responsible to support the coordination and management of impacts and consequences through provision of appropriate functional advice, leadership and information to DGS convened coordination forums, such as the Consequence Coordination Team (CCT). The advice will:

* Identify the lead executive and Incident Manager
* identify impacts
* identify actual, emergent and related consequences and related actions
* form the basis of intelligence used to brief other WoVG stakeholders
* be available to other departments and government agencies who can use this information to brief Ministers and senior staff
* provide advice on public and industry messaging.

[Person or team] is responsible to ensure adequate internal arrangements are established to enable timely and accurate reporting of consequences.

|  |
| --- |
| What do these arrangements looks like in your context? This may include activation of Privacy teams, legal teams or General Counsel, Business Continuity teams and your Media and Communications teams. |

[Person or team] is responsible to log any unresolved risks in an internal risk register, and manage in accordance with the internal risk management framework.

[Person or team] is responsible to lead engagement, as required, with relevant external stakeholders (including private industry) to support WoVG incident response and consequence management messaging.

[Person or team] is responsible to manage consequences for areas of portfolio responsibility, as defined in the State Emergency Management Plan. This is relevant during any incident, including non-emergency incidents.

[Person or team] is responsible to provide strategic and management advice about actual, emergent and cascading consequences on areas of portfolio responsibility:

* During a non-emergency incident, this will be directed to DGS’ Cyber Consequence Coordinator.
* During a cyber security emergency, this will be directed to the Emergency Management Commissioner, State Controller and/or Deputy Class 2 State Controller – Cyber Security via the State Consequence Coordinator directly, or as a part of the State Emergency Management Team.

[Person or team] is responsible to engage business continuity arrangements as required.

|  |
| --- |
| Repeat the content of above section for each consequence that you identify |

|  |
| --- |
| This content below is only relevant to Departments with a Sector Resilience Network. |

Sector Resilience Network Chair is responsible to provide information to and from industry network members to inform DGS’ decision-making.

Sector Resilience Network Chair is responsible to identify key risks and consequences to critical services.

Sector Resilience Network Chair is responsible to provide assurance to government, as appropriate.

## Relief (assistance to meet essential needs)

We are the responsible Relief Coordination Agency for [activity, refer to [Table 11: ‘Specified relief activities and relief coordinating agency’](https://www.emv.vic.gov.au/responsibilities/semp/roles-and-responsibilities/relief-services-and-co-ordination) of the State Emergency Management Plan]

We are the responsible Lead support agency for relief services for [service, refer to [Table 12: ‘Relief coordination’](https://www.emv.vic.gov.au/responsibilities/semp/roles-and-responsibilities/relief-services-and-co-ordination) of the State Emergency Management Plan]

[Person or team] is responsible to manage the delivery of these relief arrangements, including to detail the range and types of assistance, and the providers of each, to support community relief during and immediately after emergencies.

## Management Teams

Incident Management Team

The Incident Management Team:

* is activated for incidents requiring a team for an effective internal response to both technical and non-technical consequences.
* may operate on an informal basis for lower-level incidents (event, minor)
* may include as many or as few members as considered necessary

**Table X** outlines the potential membership of the internal Incident Management Team. This membership should be modified if sensitivity is needed for the particular incident, or for another reason.

Senior Executive Management Team

More serious cyber security incidents may require the formation of the Senior Executive Management Team.

The Senior Executive Management Team may form at the request of the Incident Manager, or at the discretion of the Chief Executive Officer [or Chief Information Security Officer, if more appropriate].

The Senior Executive Management Team should provide strategic oversight, direction and support to the Incident Management Team, with a focus on:

* Strategic issues identification and management
* Stakeholder engagement and communications (including ministerial liaison, if appropriate)
* Resource and capability demand (including urgent logistics or finance requirements, and human resources considerations during response effort).

If a Senior Executive Management Team does not form, the Incident Manager has the delegation to make critical decisions.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Severity level & WoVG category | |  | Standard membership of the Incident Management Team  The membership should be confirmed for each incident. | | | |  | Standard membership of the Senior Executive Management Team. The membership should be confirmed for each incident. | | | |
| **1** | **Event** | Incident manager | [Name] | [Role] | [Phone & email] | Not required | | | |
| [Other member] | [Name] | [Role] | [Phone & email] |
| **2** | **Minor** | Incident manager (ensuring routine internal procedures are followed) | [Name] | [Role] | [Phone & email] | Not required | | | |
| [Other member] | [Name] | [Role] | [Phone & email] |
| **3** | **Limited** | **Officer or executive level membership** | | | | Not required | | | |
| Incident manager (Chair) | [Name] | [Role] | [Phone & email] |  | | | |
| Chief Information Security Officer (optional) | [Name] | [Role] | [Phone & email] |
| Cyber security | [Name] | [Role] | [Phone & email] |
| I.T. team | [Name] | [Role] | [Phone & email] |
| Business continuity | [Name] | [Role] | [Phone & email] |
| Communications team | [Name] | [Role] | [Phone & email] |
| Impacted contracted service provider (if relevant) | [Name] | [Role] | [Phone & email] |
| Others as determined by the Chair (e.g. representing a particular portfolio with a consequence, a supporting contracted service provider, system administrator, network engineer, change manager, internal auditor, legal advisor, finance and procurement specialist) | [Name] | [Role] | [Phone & email] |
| Administration and recording keeping | [Name] | [Role] | [Phone & email] |
| **4**  **5**  **6** | **Major**  **Critical**  **Emergency** | **Executive level membership**  These members represent the same teams as above, however the members are, where possible, more senior representatives. | | | | **Senior executive level membership** | | | |
| Incident manager (chair) | [Name] | [Role] | [Phone & email] | Chief Executive Officer (Chair) | [Name] | [Role] | [Phone & email] |
| Chief Information Security Officer | [Name] | [Role] | [Phone & email] | Chief Information Security Officer (Deputy Chair) | [Name] | [Role] | [Phone & email] |
| Cyber security | [Name] | [Role] | [Phone & email] | Chief Information Officer | [Name] | [Role] | [Phone & email] |
| I.T. | [Name] | [Role] | [Phone & email] | Chief Operating Officer | [Name] | [Role] | [Phone & email] |
| Business continuity | [Name] | [Role] | [Phone & email] | Chief Financial Officer/Procurement Manager | [Name] | [Role] | [Phone & email] |
| Communications | [Name] | [Role] | [Phone & email] | Legal Counsel | [Name] | [Role] | [Phone & email] |
| Emergency management | [Name] | [Role] | [Phone & email] | Media and Communications Manager | [Name] | [Role] | [Phone & email] |
| Impacted contracted service provider (if relevant) | [Name] | [Role] | [Phone & email] | People and Culture Manager | [Name] | [Role] | [Phone & email] |
| Others as determined by the Chair | [Name] | [Role] | [Phone & email] |  |  |  |  |
| Administration and recording keeping | [Name] | [Role] | [Phone & email] |  |  |  |  |

[Person or team] (e.g. Incident Manager) is responsible to develop a Technical Response Incident Action Plan.

[Person or team] (e.g. Incident Manager) is responsible to activate an internal Incident Management Team to delegate particular functions to as required, to resolve the incident using local resources.

[Person or team] (e.g. Incident Manager) is responsible to perform all functions of incident management internally (as per the Australasian Inter-Service Incident Management System; see **Appendix X**).

[Person or team] is responsible to prepare and send out ‘situation updates’ **(Appendix X)** to internal stakeholders at regular intervals.

[Person or team] is responsible to maintain an ‘incident log’ **(Appendix X).**

[Person or team] is responsible to activate surge arrangements for additional people, hardware, software and financial resources.

## Operations room

The Incident Manager is responsible to determine if the incident requires a response from the dedicated operations room. The dedicated operations room is located at [room details].

[Person or team] is responsible for after-hours access [contact details].

[Person or team] is responsible for arranging catering

[Person or team] is responsible to set up the following if the response is **not** led from a dedicated on-site operations room:

* phone/teleconference/online dial-in details
* out-of-band communications (e.g. Slack or other similar applications).

## Internal communication

[Person or team] is responsible to brief all or a subset of employees (for example, all system users, customer service teams, senior executives and/or the Board) about a compromise

Internal communications will include:

* a summary of the compromise and its business impact
* actions currently being undertaken to resolve the compromise
* actions personnel can take to assist
* business continuity options for personnel who are affected
* messaging for external stakeholders
* key points of contact for enquiries
* expected timeframes for further updates.

[Communications lead and the Incident Manager, or the Senior Executive Management Team Chair if the Senior Executive Management Team is activated] is responsible to review and approval all internal communications and external media communications prior to release.

## Media and public communication

[Person or team] is responsible to authorise media content, in consultation with:

* the Department of Government Services
* Emergency Management Joint Public Information Committee (during a cyber security emergency only)
* State Control Centre Public Information Officer (during a cyber security emergency only).

[Person or role] is the nominated spokesperson, if required.

[Person or team] is responsible to consult with [the Victorian Managed Insurance Authority or other insurance provider] about how to communicate to the public, as this could impact a future insurance claim.

|  |
| --- |
| How will this spokesperson be supported? |

Media and public communication will support the Incident Management Team and Senior Executive Management Team communications requirements, and will include:

* the nature and impact of the cyber security incident
* the extent of affected systems, services or information
* the steps being taken to resolve the incident
* when systems or services are expected to return to normal (if known)
* any other information for individuals to minimise the harm of the cyber incident.

[Person or team] is responsible to monitor news media, social media and [other forms of media] to support communications.

[Person or team] is responsible to respond to ensure capacity to respond to potential increases in internal and external enquiries or complaints about compromise and is impacts.

|  |
| --- |
| How will the customer helpdesk manage enquiries and be supported?  How will the IT helpdesk manage enquiries and be supported?  What communication channels are available to affected customers (e.g. direct email, telephone hotline, information on the website or social media)?  What backup communication channels exist to communicate with stakeholders? |

[Person or team] is responsible to manage media and public communication channels.

[Person or team] is responsible to assess the risk of harm and consider notifying affected Victorians to minimise harm.5F[[6]](#footnote-7)

## Participating in a WoVG response

[The Incident Manager, senior manager or executive] is responsible to be a member of Class 2 State Control Team – Cyber Security during a cyber security emergency, when the Department of Government Services has declared a cyber security emergency. Refer to the [State Emergency Management Plan Cyber Security Sub-Plan](https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-sub-plans/state-emergency-management-plan-cyber-security-sub-plan-edition-2)for further details.

The Incident Manager is responsible to participate in the WoVG Control Team and/or WoVG Consequence Coordination Team on request, when activated. Refer to the [**State Emergency Management Plan Cyber Security Sub-Plan**](https://www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-sub-plans/state-emergency-management-plan-cyber-security-sub-plan-edition-2) for further details.

The Incident Manager is responsible to attend any control or coordination centre that is activated, when required for particular cyber security emergency activities (such as an in-person meeting).

# Recovery

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required.  Ensure that your responsibilities in the CSIMP and Sub-Plan are addressed. |

## Recovery

[Person or team] is responsible to prepare a Recovery Plan in a manner that reflects the type and severity of compromise or consequence. The Recovery Plan will be incorporated into the Incident Action Plan at **Appendix X**, in consultation with:

* business continuity
* risk team
* IT services.

[Person or team] is responsible to provide the Department of Government Services with updates on recovery progress.

|  |  |
| --- | --- |
| Environment | Relevant adverse impacts |
| Built | * cyber infrastructure which requires repair and restoration. * recovering IT and/or operational technology * impact essential utilities, services and built infrastructure. |
| Social | * death, injuries or illness * impacted psychosocial health * increased strain on the health system * difficulty making decisions without clear information * concerns about returning to ‘normal’ life * disruptions to cultural practices. * impact community cohesion, leading to social division. |
| Economic | * loss of business * loss of livelihoods * disruptions to the supply chain * unique shifts in demand. * short-term financial viability. * long-term aim is to help businesses build back up. |
| Natural | * [Direct or indirect impacts] |
| Aboriginal culture and healing | * Disruption of service provision through Aboriginal community-controlled organisations and Traditional Owner corporations * loss of data sovereignty * theft of sensitive cultural heritage information and traditional knowledge * delays in critical care * impacts on land and resource management * adverse health impacts. * Victoria’s First Peoples as targets for cybercrime, resulting in disinformation, phishing attacks and harassment relating to communities, culture or land rights. |

## Closing out an incident

[Person or team] is responsible to consider any report provided by DGS’ Cyber Incident Response Service.

[Person or team] is responsible to complete a Cyber Security Incident Report, including responsible personnel and timeframes.

The Incident Manager is responsible to stand down the Incident Management Team. If the Senior Executive Management Team is activated, the Incident Manager will request permission of the Senior Executive Management Team to close down the Incident Management Team.

## Lessons and evaluation

[Person or team] is responsible to conduct a debrief or review to document learnings after a compromise that is or exceeds level X severity.

[Person or team] is responsible gather copies of all notes taken during the response to assist the review.

[Person or team] is responsible to share relevant outcomes from the review with a wide range of stakeholders, including the Department of Government Services.

[Person or team] is responsible to monitor the implementation of actions identified out of the review, as part of continuous improvement for the benefit of future compromises.

# Appendices

|  |
| --- |
| A reminder that this guidance template is not a mandated format. Remove, replace, add and modify as required. |

1. Acronyms

Table 1: List of acronyms

|  |  |
| --- | --- |
| Acronym | Original |
| ACSC | Australian Signals Directorate’s Australian Cyber Security Centre |
| AGCMF | [Australian Government Crisis Management Framework](https://www.pmc.gov.au/publications/australian-government-crisis-management-framework-agcmf) |
| AIIMS | Australasian Inter-Service Incident Management System |
| ASD | Australian Signals Directorate |
| BCP | Business Continuity Plan |
| BIL | Business Impact Level |
| CCT | Consequence Coordination Team |
| CI | Critical Infrastructure |
| CISC | Department of Home Affairs’ Cyber and Infrastructure Security Centre |
| CIRS | Cyber Incident Response Service |
| CISO | Chief Information Security Officer |
| CSIMP | Cyber Security Incident Management Plan |
| DF | Digital Forensics |
| DGS | Department of Government Services |
| DHA | Department of Home Affairs |
| DoS/DDoS | Denial of Service/Distributed Denial of Service |
| DR | Disaster Recovery |
| E8 | ACSC’s Essential Eight Maturity Model |
| IMT | Incident Management Team |
| IR | Incident Response |
| IP | Internet Protocol |
| IRAP | Information Security Registered Assessors Program |
| ISM | Australian Government Information Security Manual |
| MSP | Managed Service Provider |
| NIST | National Institute of Standards and Technology |
| OVIC | Office of the Victorian Information Commissioner |
| PDP Act | Privacy and Data Protection Act 2014 (Vic) |
| PIO | Public Information Officer |
| PSPF | Protective Security Policy Framework |
| SITREP | Situation Report |
| SOC | Security Operations Centre |
| SOCI Act | Security of Critical Infrastructure Act 2018 (Cth) |
| SOP | Standard Operating Procedure |
| SRN | Sector Resilience Network |
| Portal | [Whole of Victorian Government Cyber Security Portal](https://vicgov.sharepoint.com/sites/VG002650/SitePages/Incident-Reporting.aspx) |
| TLP | Traffic Light Protocol |
| Victorian Government | Victorian Government |
| VicGov | Victorian Government |
| VicPol | Victoria Police |
| VMIA | Victorian Managed Insurance Authority |
| VPDSF/S | Victorian Protective Data Security Framework/Standards |
| VPF | Victorian Preparedness Framework |
| WoVG | Whole of Victorian Government |

1. Comparison of WoVG cyber security incident categories with Business Impact Levels

The Whole of Victorian Government (WoVG) cyber incident categories are prepared as a comparable state-level equivalent to the Office of the Victorian Information Commissioner’s (OVIC’s) entity-level Business Impact Levels (BILs).6F[[7]](#footnote-8)

Importantly, the 2 sets of categories do not otherwise match up with each other. For example, an entity may identify a BIL 4 ‘Serious’ incident. While treated seriously by the department or government agency, it **does not** equate to a cyber security emergency at the state level.

Table 2: Comparison between WoVG incident categories and BILs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| For use at a WoVG scale | |  | For use internally within a department or government agency7F[[8]](#footnote-9) | |
| Severity level | WoVG category | Business impact | BIL |
| 1 | Cyber security event | N/A | BIL 0 |
| 2 | Minor cyber security incident | Minor | BIL 1 |
| 3 | Limited cyber security incident | Limited | BIL 2 |
| 4 | Major cyber security incident | Major | BIL 3 |
| 5 | Critical cyber security incident |
| 6 | Cyber security emergency | Serious | BIL 4 |
| Exceptional | BIL 5 |

1. Assets and key contacts

|  | Assets | Comment | Key Contact |
| --- | --- | --- | --- |
| Site information | IP subnet |  |  |
| DHCP scope |  |  |
| Core router IP |  |  |
| DNS servers (internal) / logs & locations |  |  |
| DNS name / logs & location |  |  |
| Secondary DNS name (external) |  |  |
| Internet connection / communications | Internet service providers IP & connection details |  |  |
| Network provider IP & connection details |  |  |
| VOIP / PABX phone system details IPs & number range |  |  |
| Fixed line services & hardware |  |  |
| 3g/4g mobile data services & hardware |  |  |
| Satellite phone services & hardware |  |  |
| Single point of failure analysis – communications infrastructure |  |  |
| Firewall & security | Firewall software / hardware |  |  |
| Wired network |  |  |
| Wireless network |  |  |
| Single point of failure – firewall infrastructure |  |  |
| Site remote access | Remote access methods / logs & locations |  |  |
| Single point of failure analysis – remote access infrastructure |  |  |
| Wired network switch infrastructure | Hardware / firmware / logs & locations |  |  |
| Single point of failure analysis |  |  |
| Wireless network switch infrastructure | Hardware / firmware / logs & locations |  |  |
| Single point of failure analysis |  |  |
| Industrial control systems / SCADA infrastructure | Scada plc RTU hardware / firmware / logs & locations |  |  |
| Authentication methods & controls |  |  |
| Functional analysis |  |  |
| Process flow diagram |  |  |
| Configuration backup schedule / locations |  |  |
| Alert / alarm systems & thresholds |  |  |
| Single point of failure analysis |  |  |
| Data backup | Backup software |  |  |
| Backup location & restoration timeframes |  |  |
| Data retention requirements |  |  |
| Disaster recovery plan | Identified high availability? (yes / no) |  |  |
| Required up time (%) |  |  |
| Required return to operation (hrs) |  |  |
| Redundant power supply / UPS infrastructure | UPS hardware / location |  |  |
| Battery capacity / run time |  |  |
| Connected devices |  |  |
| Redundant power supply / generator infrastructure | Generator hardware / location |  |  |
| Fixed or portable |  |  |
| Capacity (KVA) |  |  |
| Fuel type / capacity (l) |  |  |
| Fuel consumption (l/hr) |  |  |
| On site fuel storage (l) & locations |  |  |
| Fuel supply arrangements / agreements |  |  |
| Documented fail over / restoration of services. |  |  |
| Administration systems (supporting ICT systems) | Web proxy server details / logs & locations |  |  |
| Domain controller details / logs & locations |  |  |
| Web server details / logs & locations |  |  |
| Server environment operating system details / logs & locations |  |  |
| Virtual server host environment details / logs & locations |  |  |
| Email systems | Email server details / logs & locations |  |  |
| Database systems | Server details / logs & locations |  |  |
| Production database details / logs & locations |  |  |
| Test database details / logs & locations |  |  |
| Cloud service providers | Hosted service providers & SLAS |  |  |
| Staff desktop / laptop / tablet systems | Client environment OS / logs & locations |  |  |
| Client hardware manufacturer / model |  |  |

|  |
| --- |
| Consider adding additional rows as required. E.g. HVAC, card readers and physical security, solar, CCTV and security/alarm systems, building management/maintenance contacts |

1. Supporting procedures and playbooks

### Standard Operating Procedures

|  |  |  |
| --- | --- | --- |
| Standard Operating Procedure | Physical location | Electronic location |
| Event detection, triage and analysis |  |  |
| Post event/incident detection or notification |  |  |
| Incident detection, investigation and analysis |  |  |
| Incident containment, remediation and recovery |  |  |
| Communications Plan (internal and external) |  |  |
| Emergency Management Plan |  |  |
| Crisis Management Plan |  |  |
| Business Continuity Plan |  |  |
| Disaster Recovery Plan |  |  |

### Playbooks

Playbooks are documents with easy-to-follow instructions to assist in ensuring all appropriate steps are taken when responding to specific types of compromises.

|  |  |  |
| --- | --- | --- |
| Playbook | Physical location | Electronic location |
| Phishing |  |  |
| Data Breach/Theft |  |  |
| Malware |  |  |
| Ransomware |  |  |
| Denial of Service |  |  |
| Supply Chain Incident |  |  |
| Consider others, such as: insider threat and physical access |  |  |

1. Incident Action Plan Template

**Incident Action Plan for [Incident name]**

This template must be modified as much as required to reflect the magnitude of the incident.

|  |  |
| --- | --- |
| Version control |  |
| Version #X | Date and time of version |
| Next update | Date and time of next update |
| Author |  |
| Approved for distribution by | Incident Manager |
| Distribution | List of people the plan is provided to |
| Incident folder | Reference the folder where incident documentation is kept |

|  |  |
| --- | --- |
| Key technical incident details – current state | |
| Incident Status | New, In Progress, Resolved |
| Classification | Event / Minor / Limited / Major / Critical / Emergency |
| Incident type | e.g. ransomware / denial of service / data breach / malware / phishing / social engineering |
| Threat actor |  |
| Scope | What we know & what we don’t yet know  List the affected systems, services and/or networks; highlight any change to scope since the previous version.  e.g. for data breach:   * type of data exposed * volume of data exposed * internal impact * impact on public safety or services * Was it a misconfiguration/error, or malicious exfiltration, theft? |
| Impact, severity and estimated time of restoration |  |
| Predictions of likely development/s |  |

|  |  |  |
| --- | --- | --- |
| Environment | Non-technical consequence/s | Prediction of likely development/s |
| Social environment |  |  |
| Built environment |  |  |
| Economic environment |  |  |
| Natural environment |  |  |
| Natural environment |  |  |

|  |  |
| --- | --- |
| Incident objective/s | |
| Objective 1 | What we want to achieve, and when.  Consider objectives that relate to:   * Technical response * Non-technical consequences |
| Objective 2… | * What we want to achieve, and when. * Consider objectives that relate to: * Technical response   Non-technical consequences |

|  |  |  |
| --- | --- | --- |
| Incident Management Team | Current rotation, including contact details | Next rotation, including starting date |
| Incident Controller |  |  |
| Chief Information Security Officer (optional) |  |  |
| Cyber security team |  |  |
| I.T. team |  |  |
| Business continuity |  |  |
| Communications team |  |  |
| Impacted contracted service provider (if relevant) |  |  |
| Others? |  |  |
| Administration and recording keeping |  |  |

|  |  |  |
| --- | --- | --- |
| State Executive Management Team | Member | Alternate contact |
| Chief Executive Officer (Chair) |  |  |
| Chief Information Security Officer (Deputy Chair) |  |  |
| Chief Information Officer |  |  |
| Chief Operating Officer |  |  |
| Chief Financial Officer/Procurement Manager |  |  |
| Legal Counsel |  |  |
| Media and Communications Manager |  |  |
| People and Culture Manager |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Notifications | When notified | How notified | Key contact |
| Stakeholder to be notified  Refer to the notification section of the plan.  (e.g. ASD, law enforcement, OAIC, customers, media) |  |  |  |
| DGS’ Cyber Incident Response Service | e.g. Tuesday 17th, 3:45pm | e.g. Whole of VicGov Portal |  |
|  |  |  |  |

|  |  |
| --- | --- |
| Incident timeline |  |
| Key date/time | Incident first detected: detail on what was observed (e.g. the sequence of events, date/time, effect/event, who observed it) |
| Key date/time |  |
| Key date/time |  |
| Key date/time |  |

|  |  |
| --- | --- |
| External assistance | Provider |
| What assistance is currently required, requested, or being provided from other department or agencies? | For example:   * Incident response provider * DGS’ Cyber Incident Response Service * ASD * law enforcement |
|  |  |

|  |  |
| --- | --- |
| Public communication |  |
| Summary |  |
| Media interest |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Meetings held/to be held | Time/Day | Chair | Minute taker | Participants | Next meeting |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Products developed | Link | Audience | Time/Day delivered to audience | Next product due |
| Incident Log |  |  | Ongoing access available |  |
| Evidence Register |  |  | Ongoing access available |  |
| XX |  |  | Tuesday 17, via email |  |
|  |  |  |  |  |

|  |  |
| --- | --- |
| Attachments | Link |
| Cyber Security Incident Response Plan |  |
| Victorian Government Cyber Security Incident Management Plan |  |
| Standard Operating Procedures: X |  |
| Playbook: X |  |

| # | Relevant incident objective/s | Action | Priority | Action Owner | Resources | Communication requirements | Expected completion date | Status | Notes/ Comments |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 |  | containment |  |  |  |  |  | Complete |  |
| 2 |  | eradication |  |  |  |  |  | In Progress |  |
| 3 |  | approach to recovering IT networks, systems and applications |  |  |  |  |  | Not yet started |  |
| 4 |  | restore systems to normal operation |  |  |  |  |  |  |  |
|  |  | continual monitoring to confirm that the affected systems are functioning normally |  |  |  |  |  |  |  |
|  |  | criminal investigation (including forensic evidence collection). |  |  |  |  |  |  |  |
|  |  | Test systems/services to ensure the threat has been eradicated and affected systems/services are back to normal function |  |  |  |  |  |  |  |
|  |  | stakeholder communication |  |  |  |  |  |  |  |
|  |  | Implement disaster recovery arrangements to return impacted systems and services to normal operation as soon as possible |  |  |  |  |  |  |  |
|  |  | systems, services and networks be monitored to ensure they are no longer compromised or functioning as expected |  |  |  |  |  |  |  |
|  |  | Monitoring for impacted natural and cultural heritage values, in consultation with affected communities, including Victoria’s First Peoples and Traditional Owner groups. |  |  |  |  |  |  |  |
|  |  | Liaise with Victorian Managed Insurance Authority or other insurance provider to determine what support for recovery is available |  |  |  |  |  |  |  |

1. Incident Log Template

The incident log should capture minutes from each IMT meeting, details of all critical decisions (including the rationale for a decision), operational actions taken, action items and future meeting dates and times.

| Date | Time | Author | Notes (relevant facts, decisions, rationale) |
| --- | --- | --- | --- |
| 20220330 | 0835hrs |  | SOC identified phishing that resulted in the successful deployment of ransomware to the system. |
| 20220331 | 1455hrs |  | CSIRT collected forensic artefacts (listed in the Evidence Register). An initial investigation has assessed the cyber security incident as ‘High’.  The following systems are currently offline: ... |
| 20220401 | 1150hrs |  | SEMT voted to escalate the cyber security incident to ‘Critical’.  Next actions were agreed to as follows: … |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

## 

1. Evidence Register Template

This should include who collected or handled the evidence, the time and date (including time zone) evidence was collected and handled, and the details of each item collected (including the physical location, serial number, model number, hostname, media access control [MAC] address, Internet Protocol [IP] address and hash values).

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Date of Collection | Time collected (and time zone) | Location of collection | Collected by name and role | | Item Details8F[[9]](#footnote-10) | Storage Location | Label Number | Access date | Access time | Person who accessed and role | | Reason for access after collection |
| 20220402 | 1200hrs | Head Office | Jane Doe | CSIRT | 1 x disk & memory image, XYZ Desktop, ABC Model Number, IP ###.###.###.###, ... | Stored on hard drive in IT Security Office and on network drive H:\... | asset number #### |  |  |  | CSIRT team | law enforcement, ASD |

1. Analysis questions

Cyber security incident analysis is broken into the following categories:

* **Protection:** Identifies the control mechanisms that were in place at the time of the cyber security incident and their effectiveness. Establishes how to improve the protection of systems, services and networks.
* **Detection:** Establishes how to reduce the time to identify a cyber security incident. Addresses what detection mechanisms were in place and how those mechanisms could be improved.
* **Response:** Identifies improvements for the response.
* **Recovery:** Addresses improvements for recovery.

|  |  |
| --- | --- |
| Protection | |
| What controls were in place that were expected to stop a cyber security incident similar to this? |  |
| How effective were those controls? | Did they work? Why/why not?  How could they be improved? |
| Are there other controls considered better for protecting against a similar cyber security incident? | What are they? |
| What business processes and procedures were in place to prevent this type of cyber security incident from occurring? |  |
| How effective were those business processes and procedures? | Did they work? Why/why not?  How could they be improved? |
| Any other findings and/or suggestions for improvement in the following areas?   * **People:** Roles, responsibilities, accountabilities, skills. * **Process:** Plans, policies, procedures, protocols, processes, templates, arrangements. * **Department or agency:** Structures, culture, jurisdictional arrangements. * **Support:** Infrastructure, facilities, maintenance. * **Technology:** Equipment, systems, standards, security, inter-operability. * **Training:** Qualifications/skill levels, identification of required courses. * **Exercise management:** Exercise development, structure, management, conduct. |  |
| PROPOSED ACTIONS | Detail any resulting actions that can be incorporated into the Incident Action Plan.  Summary of action and responsible action owner. |

|  |  |
| --- | --- |
| Detection | |
| How was the incident detected? | How did the department or agency know a cyber security incident was happening? |
| What controls were in place to detect the incident? |  |
| Were those controls effective? | Did they work? Why/why not?  How could they be improved? |
| Are there any ways to improve the ‘time to detection’? | How could the department or agency reduce that time? |
| Are there any indicators that can be used to detect similar incidents in the future? |  |
| Are there any additional tools or resources that are required in the future to detect similar incidents? | Is there anything from a detection perspective that would help mitigate future cyber security incidents? |
| Any other findings and/or suggestions for improvement? | What activities worked well? What activities did not work so well? What could be changed with hindsight?  See the PPOSTTE model for guidance. |
| PROPOSED ACTIONS | Detail any resulting actions that can be incorporated into the Incident Action Plan.  Summary of action and responsible action owner. |

|  |  |
| --- | --- |
| Response | |
| What was the cause of the incident? |  |
| What was the initial intrusion vector? |  |
| How was the incident resolved? | What needed to happen? |
| What post-exploitation activity occurred? What accounts were compromised? What level of privilege was involved? |  |
| Does the malicious actor have persistence on systems, services or networks? |  |
| Is lateral movement suspected or known? Where has the malicious actor laterally moved to and how? |  |
| How is the malicious actor maintaining command and control? |  |
| Has data been accessed or exfiltrated and, if so, what kind of data? |  |
| What business processes and procedures were used in responding to the cyber security incident, and were they effective? | E.g. following the CSIRP worked very well. |
| What delays and obstacles were experienced when responding? |  |
| Were there any escalation points? | Were there any escalation points that the cyber security incident went through? |
| If there were escalation points, did they hamper the response or were they at the appropriate level? | For example, having to escalate to a Chief Operating Officer to take action on an ongoing cyber security incident had severe timeline impacts for the response. |
| How well did the information sharing and communications work within your department or agency? | What worked well/what did not work well? How could it be improved?  Was there any information that was needed sooner?  How did the department or agency communicate within the IR team, across jurisdictions, across time zones, legal teams and external comms teams? |
| Were there any media enquiries received during the cyber security incident? | If yes, how did the department or agency respond? |
| Was media produced during the cyber security incident? | If yes, what was the media that was produced? |
| Were stakeholders and/or customers notified during the cyber security incident? | Why/why not? When? How?  Was it effective? How could it be improved? |
| Were trained personnel available to respond? | Are there any personnel knowledge and/or skills gaps? What are they?  Were there enough resources available to respond? |
| Any other findings and/or suggestions for improvement? | See the PPOSTTE model for guidance. |
| PROPOSED ACTIONS | Detail any resulting actions that can be incorporated into the Incident Action Plan.  Summary of action and responsible action owner. |

|  |  |
| --- | --- |
| Recovery | |
| How long did it take for all systems, services and networks to recover? |  |
| How could this time be improved? | For example, how could the recovery time be reduced? |
| Are there any obligations to report externally about the cyber security incident? | If yes, to who? |
| Were there any media enquiries after the cyber security incident? | If yes, how did the department or agency respond? |
| Were stakeholders and/or customers notified following the cyber security incident? | Why/why not? When? How?  Was it effective? How could it be improved? |
| Any other findings and/or suggestions for improvement? | See the PPOSTTE model for guidance. |
| PROPOSED ACTIONS | Detail any resulting actions that can be incorporated into the Incident Action Plan.  Summary of action and responsible action owner. |

1. Post incident reviews

A post incident review is a detailed review conducted after an incident. The review focuses on providing recommended actions to mitigate future incidents.

Post cyber security incident debriefs are useful for capturing observations from personnel directly involved in managing a cyber security incident and identifying actions to improve how their department or agency managed its response, as well as how the cyber security incident could have been prevented.

There are two types of debriefs: Hot debriefs and Formal debriefs (cold debriefs).

|  | Hot Debrief | Formal debrief (Cold debrief) |
| --- | --- | --- |
| Summary | * those involved can provide instant feedback and lessons learned * urgent issues can be addressed immediately * those involved are more likely to recall information and detail as it is still fresh in their minds. | * provides opportunity to discuss the incident in detail, gather key insights, learnings and opportunities for improvement. * ensures all key personnel are present, including senior management. |
| When | Immediately after the incident. | Days to weeks after the incident, after emotions and stress have settled |
| Recommended time | 30 minutes to 1 hour | 1–2 hours |
| Aim | 1. review the incident 2. receive observations and insights 3. identify urgent issues requiring immediate action | 1. review the incident 2. analyse the root cause 3. identify remaining vulnerabilities 4. validate what worked 5. identify what can be improved, and assign actions that will ensure this improve. |
| Participants | 1. facilitator (such as a manager who was involved during the cyber security incident) 2. a scribe. 3. IMT 4. all other personnel involved except senior executives.   Senior executives should NOT be present, to ensure free and open conversation. | 1. facilitator (such as a manager who was involved during the cyber security incident) 2. a scribe. 3. IMT 4. SEMT 5. Senior executives should be present, who will drive the implementation of actions. 6. all other personnel involved, including:    1. technical personnel who were involved in detecting, responding to and resolving the cyber security incident    2. non-technical personnel who were involved during the cyber security incident    3. communications/media personnel involved in the cyber security incident. |
| Ground rules | * Everyone is encouraged to share thoughts and ideas * Respond using your knowledge regardless of how much or little you know. * No fault systems-focus: examine systems of work rather than individual performance * Respect others, all views are welcome and valued, including differing opinions | |
| Agenda | * Provide a summary of exactly what happened and when. * What went well? * What could we do differently next time to improve? * What action has been taken to remediate immediate risk? * How could the incident have been prevented? * Are there any further issues that require immediate resolution? * Conclusion: A summary of the discussion to participants to confirm whether the key issues and actions were captured. * Next steps and expected timeframes. * How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate? * What information was needed sooner? * Were any steps or actions taken that might have inhibited the recovery? * How could information sharing with other department or agencies have been improved? * What corrective actions can prevent similar incidents in the future? * What training activities or additional support would be useful, to help you respond to a similar incident in future? * What precursors or indicators should be watched for in the future to detect similar incidents? * What additional tools or resources are needed to detect, analyse, and mitigate future incidents? | |
| Post review activity | Document actions in the Incident Action Plan. | Document actions in the Incident Action Plan.  Complete the Post Cyber Security Incident Review Analysis.  Circulate both to participants and action owners for feedback.  Once feedback is incorporated, seek endorsement of the responsible executive.  Submit action progress reporting at agreed intervals. |

1. This relates specifically to VPDSF/S Standard 6, to ‘establish, implement and maintain an information security incident management process relevant to size, resources and risk posture.’ [↑](#footnote-ref-2)
2. Section 88 of the *Privacy and Data Protection Act 2014* (Vic). [↑](#footnote-ref-3)
3. In line with ACSC’s guidance regarding the Essential 8, departments and government agencies may consider additional mitigation strategies and controls can be considered, including those from the [*Strategies to Mitigate Cyber Security Incidents*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents) and the [*Information Security Manual*](https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism). [↑](#footnote-ref-4)
4. **IMPORTANT:** Do not ‘ping’ or try to communicate with a suspected IP address or URL from your own network. This may tip off the attacker that you have detected their activity. A contracted service provider can conduct this activity securely and anonymously. [↑](#footnote-ref-5)
5. Refer to the Victorian Government Log Collection and Retention Guidelines, available from DGS. [↑](#footnote-ref-6)
6. Refer to OVIC’s guide to [Managing the Privacy Impacts of a](https://ovic.vic.gov.au/book/managing-the-privacy-impacts-of-a-data-breach/) [Data Breach](https://ovic.vic.gov.au/book/managing-the-privacy-impacts-of-a-data-breach/). [↑](#footnote-ref-7)
7. VPDSF BILs, Version 2.1, November 2019. [↑](#footnote-ref-8)
8. While the requirements surrounding BILs of the VPDSF are not applicable to councils (except in some instances where the council may act as Committee of Management for Crown Land Reserves), councils may optionally consider BILs in their own cyber security arrangements. [↑](#footnote-ref-9)
9. Quantity, serial number, model number, hostname, MAC address, IP addresses, hash values [↑](#footnote-ref-10)