State Emergency Management Plan Cyber Security Sub-Plan

For cyber security emergencies

March 2024

VICTORIA State Government | Government Services

Produced and published by

This State Emergency Management Plan Cyber Security Sub-Plan (the Plan) has been prepared by the Department of Government Services as the Control Agency for cyber security emergencies, on behalf of the Emergency Management Commissioner. The Plan was approved by the State Crisis and Resilience Council on 29 November 2023.

Authorised and published by the Victorian Government Melbourne
March 2024

Acknowledgement: Page i photo by Krzysztof Hepner on Unsplash
Page ii photo by Markus Spiske on Unsplash
Page 4 photo by Phillip Katzenberger on Unsplash
Page 14 photo by Chris Liverani on Unsplash
Page 42 icon created by Un.delivered on Noun Project
Page 69 photo by Anas Alshanti on Unsplash

This document is available in accessible format at www.emv.vic.gov.au/responsibilities/state-emergency-management-plan-sub-plans.

ISBN 978-1-925789-99-7 (PDF/online/MS Word)

Contents

Acronyms

This Plan uses full references instead of acronyms to support readability. However, in the event of a compromise of cyber security, acronyms are commonly used. **Appendix A's** table of acronyms is prepared to support the reader's understanding in these contexts.

Version

This is the third version of a state-level plan addressing cyber security emergency arrangements. The first two versions were prepared by the Department of Premier and Cabinet as the then-Control Agency for cyber security emergencies.

On 1 January 2023, the Victorian Government established the Department of Government Services, with its responsibilities including a transfer of Control Agency from the Department of Premier and Cabinet. This Sub-Plan demonstrates that the Department of Government Services continues to expand the scope of cyber security activities that were previously provided by the Department of Premier and Cabinet.

This version of the Plan builds on the version it supersedes, which was the first hazard-specific sub-plan developed under a reformed emergency management planning framework.

This third version of the plan is prepared within a context of greater maturity of both Victoria's emergency management planning framework, and Whole of Victorian government cyber security arrangements.

Acknowledgment of Country

The Department of Government Services acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of the land.

The Department of Government Services also acknowledges and pays respect to the Elders, past and present and is committed to working with Aboriginal and Torres Strait Islander communities to achieve a shared vision of safer and more resilient communities.

Plan activation

This Plan is current at the time of publication and remains in effect until modified, superseded or withdrawn.

The arrangements in this Plan apply on a continuing basis and do not require activation.

1 Introduction

1.1 Early response summary

This high-level summary outlines the first steps required from the point of detection. This section is a quick reference guide to support an efficient response.

TABLE 2: Summary of early response steps

Early response step number	Process	Summary	Where responsibilities for this step are outlined
1	Detection	Identify a potential cyber security compromise	Page 23 Page 55 **(Appendix B)**
2	Analysis	Confirm whether the cyber security compromise has occurred or is likely to occur	Page 25
3	Notification	Make notifications as soon as possible and within prescribed timeframes after confirming the existence of an incident or threat.	Page 26 Page 63 **(Appendix H)**
4	Classification	Categorise the threat or incident based on the nature of the compromise and its potential impacts.	Page 28
5	Determine the relevant plan to use	Address the threat or incident using the relevant plan/s, based on the classification provided in the previous step. Refer to this plan for: → cyber security emergencies.	The Department of Government Services' Cyber Incident Response Service will advise how to proceed through the remainder of the emergency response and recovery, outlined in this Plan.

1.2 Whole of Victorian Government cyber security event, incident and emergency categories

This table outlines the categories of cyber security events, incidents and emergencies.

TABLE 1: Whole of Victorian Government cyber security event, incident and emergency categories.

Severity level	Whole of Victorian Government category	Common characteristics for a Whole of Victorian Government cyber security event, incident or emergency	Authority to declare the category	Relevant internal plan	Whole of Victorian Government plan	Notification requirement
1	**Cyber security event**	A suspected or unconfirmed cyber security event that involves: → no impact to systems, services or information (e.g., malicious scanning activity). Alternatively, a cyber security event or threat that: → does not impact or have consequences for any department or government agency, council, critical infrastructure owner or operator, or contracted service provider to departments, government agencies or councils.	Within the entity at the centre of the event or incident	Entity's internal cyber security incident response plan equivalent	No Whole of Victorian Government plan	No notification to the Cyber Incident Response Service required[1]
2	**Minor cyber security incident**	A minor cyber security incident involves: → successful compromise of cyber security with minor impact to services, information, assets, reputation, or relationships → response by routine internal procedures, within normal capability and capacity, and no additional resources or coordination required → an expectation that the incident will not spread to another entity which is a department, government agency, council, critical infrastructure owner or operator, or contracted service provider to departments, government agencies or councils.				

[1] There are some instances where the Cyber Incident Response Service may ask stakeholders to report back on findings relating to incidents of this severity for intelligence sharing purposes (for example, during a threat hunt).

Table continues next page.

Table of contents

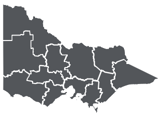
3	**Limited cyber security threat or incident**	A limited cyber security incident involves: → successful compromise of cyber security with limited impact to services, information, assets, government reputation, relationships and/or the Victorian community → reduced or impeded efficiency and effectiveness of critical infrastructure or essential services → disruption to emergency service activities requiring re-prioritisation at the local levels to meet expected levels of service → potential to spread to an entity which is a department, government agency, council, critical infrastructure owner or operator, or contracted service provider to departments, government agencies or councils. Alternatively, a cyber security threat that involves: → a major scheduled event which may be an attractive target for cyber attack → information or intelligence that identifies a low likelihood but high impact threat that warrants increased monitoring and analysis.	Manager, Cyber Incident Response Service or Victorian Government Chief Information Security Officer	Entity's internal cyber security incident response plan equivalent	Cyber Incident Management Plan (takes precedence)	Notification to the Cyber Incident Response Service required
4	**Major cyber security threat or incident**	A major cyber security incident involves: → successful compromise of cyber security with major impact to services, information, assets, government reputation, relationships and/or the community → ineffectiveness of critical infrastructure or essential services → disruption to emergency service activities requiring re-prioritisation at the entity-level to meet expected levels of service → more than one department, government agency, council, critical infrastructure owner or operator, or contracted service provider to departments, government agencies or councils → a large-scale data breach. Alternatively, a cyber security threat that involves: → information or intelligence that warrants immediate monitoring and analysis.				
5	**Critical cyber security incident**	A critical cyber security incident involves: → successful compromise of cyber security with significant impact to services, information, assets, government reputation, relationships and/or the community → sustained disruption to critical infrastructure or essential services → malicious cyber activity where the cause and potential extent of its geographic impact is uncertain → an organisation with links across multiple departments, government agencies, councils, critical infrastructure owners or operators, or contracted service providers to departments, government agencies or councils → a large-scale data breach of sensitive data.	Victorian Government Chief Information Security Officer	Entity's internal cyber security incident response plan equivalent	Cyber Incident Management Plan (takes precedence)	Notification to the Cyber Incident Response Service required
6	**Cyber security emergency**	A cyber security emergency is a serious or exceptional compromise of cyber security that must also include potential to cause or is causing: → loss of life or serious injuries → extensive damage to property, infrastructure or the environment → significant adverse consequences for the Victorian community or a part of the Victorian community → widespread disruption to, and/or damage or destruction of critical infrastructure → disruption to emergency service activities requiring re-prioritisation to meet expected levels of service → large-scale economic consequences for Victoria.	Control Agency Officer in Charge (Secretary, Department of Government Services)	Entity's internal cyber security incident response plan equivalent	**This Plan** (takes precedence)	Notification to the Cyber Incident Response Service required

2 State Emergency Management Plan Cyber Security Sub-Plan

2.1 Our collective cyber security vision

Cyber security emergencies are a direct challenge to Australia's national security, economy, environment and sense of community safety.

The Australian Government's 2023–2030 Australian Cyber Security Strategy (the Strategy) positions Australia as a world-leading cyber secure and resilient nation by 2030. The Strategy promotes sovereign capability and will take a whole-of-nation approach to building cyber resilience.



At a state level, the vision of Victoria's Cyber Strategy 2021 is to create a cyber safe Victoria. The vision is achieved through three core missions:

- the safe and reliable delivery of government services
- a cyber safe place to work, live and learn
- a vibrant cyber economy.

2.2 Shared responsibility

This Plan recognises that building cyber safe and more resilient communities is a shared responsibility.

A commitment to shared responsibility for cyber security recognises that:

- everyone has a responsibility to understand and reduce their cyber security risk
- partnerships between government, industry, community and academia are key to advancing and protecting Victoria's interests online.

Table of contents

2.3 About this Plan

2.3.1 Arrangements for cyber security emergencies

This Plan outlines Victorian Government's arrangements in the event of a cyber security emergency. This includes roles and responsibilities, and provisions providing for the mitigation of, preparation for, response to and recovery from cyber security emergencies.

This Plan is a sub-plan to Victoria's State Emergency Management Plan and is prepared with consideration to the Minister for Emergency Services' Guidelines for Preparing State, Regional and Municipal Emergency Management Plans.

Each entity should print at least one copy of this Plan for reference in the event that internal accessibility is compromised.

TIMELINE

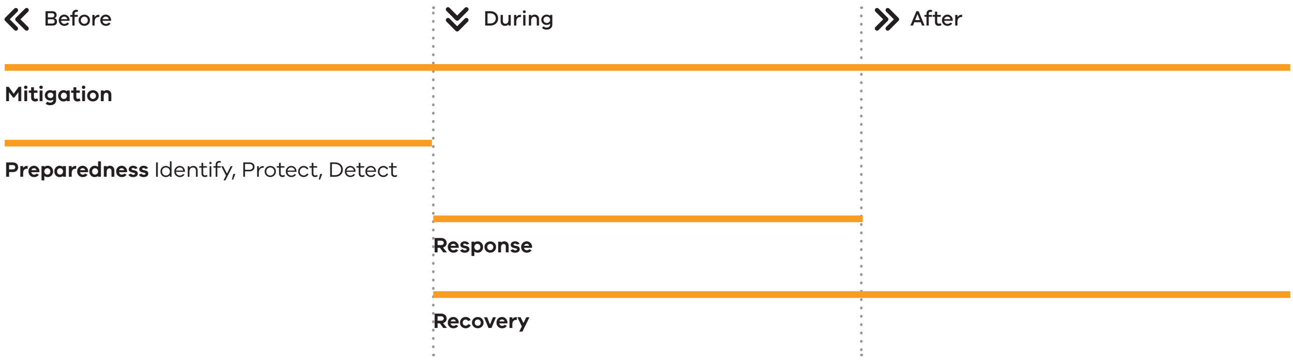


FIGURE 1: Phases across an emergency time line

2.3.2 Arrangements for non-emergency cyber security incidents

This Plan complements Victoria's equivalent arrangements for non-emergency cyber security incidents (limited, major or critical non-emergency cyber security incidents), outlined in the Cyber Incident Management Plan. These two plans share many similarities, especially across introductory, mitigation and preparedness sections.

Arrangements for cyber security events or minor cyber security incidents do not require a Whole of Victorian Government approach. They are the responsibility of each entity to determine.

2.3.3 Multiple plans ensure tailored arrangements for incidents and emergencies

Victoria's arrangements for responding to cyber security incidents and emergencies comprise three levels of plans. Each reflects an appropriate level of effort depending on the severity of the compromise of cyber security.

TABLE 3: Overview of entity and Whole of Victorian Government cyber security plans

	Entity specific cyber security incident response plan	Cyber Incident Management Plan	This Plan
Context	Supports the impacted entity to lead its response to cyber security events, incidents and emergencies	Supports the Department of Government Services leadership in Whole of Victorian Government cyber security incidents	Supports the Department of Government Services and Emergency Management Commissioner's leadership in cyber security emergencies
Prepared by, or on behalf of	The relevant entity	The Victorian Government Chief Information Security Officer	The Department of Government Services as the Control Agency for cyber security emergencies, on behalf of the Emergency Management Commissioner. The Plan is prepared as one of 13 emergency-specific sub-plans of the State Emergency Management Plan under Victoria's Emergency Management Planning Framework (Emergency Management Act 2013)
Content	Encouraged to reflect the same structure and core content as the Cyber Incident Management Plan and State Emergency Management Plan Cyber Security Sub-Plan, to enable as much consistency as possible across the arrangements for all cyber security incidents and emergencies	Reflects the same structure and core content as the State Emergency Management Plan Cyber Security Sub-Plan, to enable as much consistency as possible across the arrangements for all cyber security incidents and emergencies	Required by the Minister for Emergency Services' Guidelines for Preparing State, Regional and Municipal Emergency Management Plans to outline provisions for mitigation, response and recovery, as well as roles and responsibilities

Table of contents

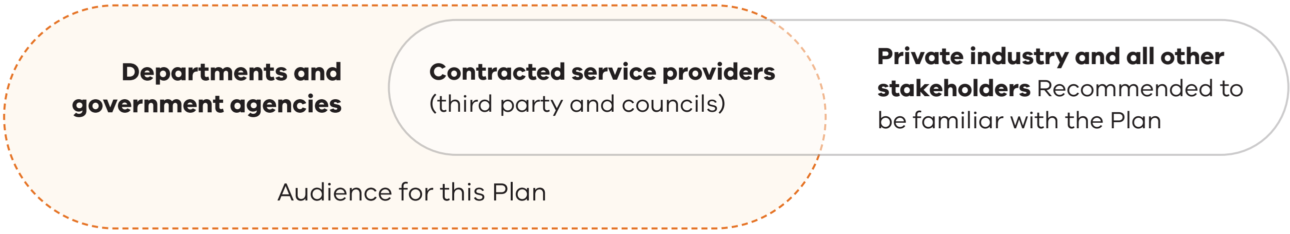

Departments and government agencies
Contracted service providers (third party and councils)
Private industry and all other stakeholders Recommended to be familiar with the Plan
Audience for this Plan

FIGURE 2: Overview of how each entity interfaces with this Plan

2.4 Audience

2.4.1 Departments and government agencies

For the purposes of this Plan, the collective term 'departments and government agencies' encapsulates Victorian:

- public service bodies, including all Victorian Government departments
- government agencies
- public entities[2]
- special and exempt bodies except for councils (see sub-section 2.4.1.5)[3]
- public sector critical infrastructure owners and operators.[4]

Departments and government agencies are responsible for ensuring contracted service providers (including managed service providers) are managing cyber security risks commensurate with the value of the information or service (for example, through contractual clauses).

2.4.2 Department of Government Services

The Department of Government Services carries additional responsibilities due to its leadership role in Victoria's cyber security arrangements. In many cases, these responsibilities are most relevant to the department's:

- Cyber Incident Response Service
- Victorian Government Chief Information Security Officer
- Class 2 State Controller – Cyber Security
- Secretary/Control Agency Officer in Charge.

2.4.3 Contracted service providers to departments and government agencies ('third parties')

In line with contractual responsibilities, third parties are required to cooperate with the arrangements in this Plan. This is especially relevant for contracted service providers that work with systems, services or information on behalf of a government department or government agency in Victoria. This Plan already applies to all contracted service providers that are also Victorian public sector bodies (for example, Cenitex).

[2] As defined in section 5 of the *Public Administration Act 2004.*

[3] As defined in section 4 of the *Public Administration Act 2004.*

[4] As designated under Victoria's *Emergency Management Act 2013,* not the Commonwealth *Security of Critical Infrastructure Act 2018.*

Table of contents

2.4.4 Private industry entity

Private industry entity includes:

- private critical infrastructure owners and operators
- businesses
- non-government community service organisations or providers
- not-for-profit organisations.

This Plan acknowledges the role of federal legislation and regulation relating to cyber security obligations for private industry, including those contained in the *Privacy Act 1998* (Cth) and the *Security of Critical Infrastructure Act 2018* (Cth).

While cooperation with this Plan is encouraged, it remains optional for private industry entities to consider this Plan, except:

- where this Plan summarises responsibilities from other authoritative sources (for example, Commonwealth or Victorian legislation), or
- where the private industry entity is a contracted service provider to the Victorian Government, with contractual cyber security responsibilities.

In all other instances, private industry entities should become familiar with this Plan when experiencing a compromise of cyber security that in any way interfaces with or has consequences relevant to Victorian departments and government agencies. For scenarios such as these, this Plan recommends actions for private industry entities to consider.

2.4.5 Councils

Victoria's councils are encouraged to adopt this Plan.

Throughout this Plan there are instances which reflect the arrangements available to support councils. Each council is encouraged to consider these arrangements in their own internal cyber security planning, or in any multi-agency emergency management municipal or regional planning.

Councils may consider any reference to 'departments and government agencies' as applicable for their purposes where relevant.

2.4.6 Other stakeholders

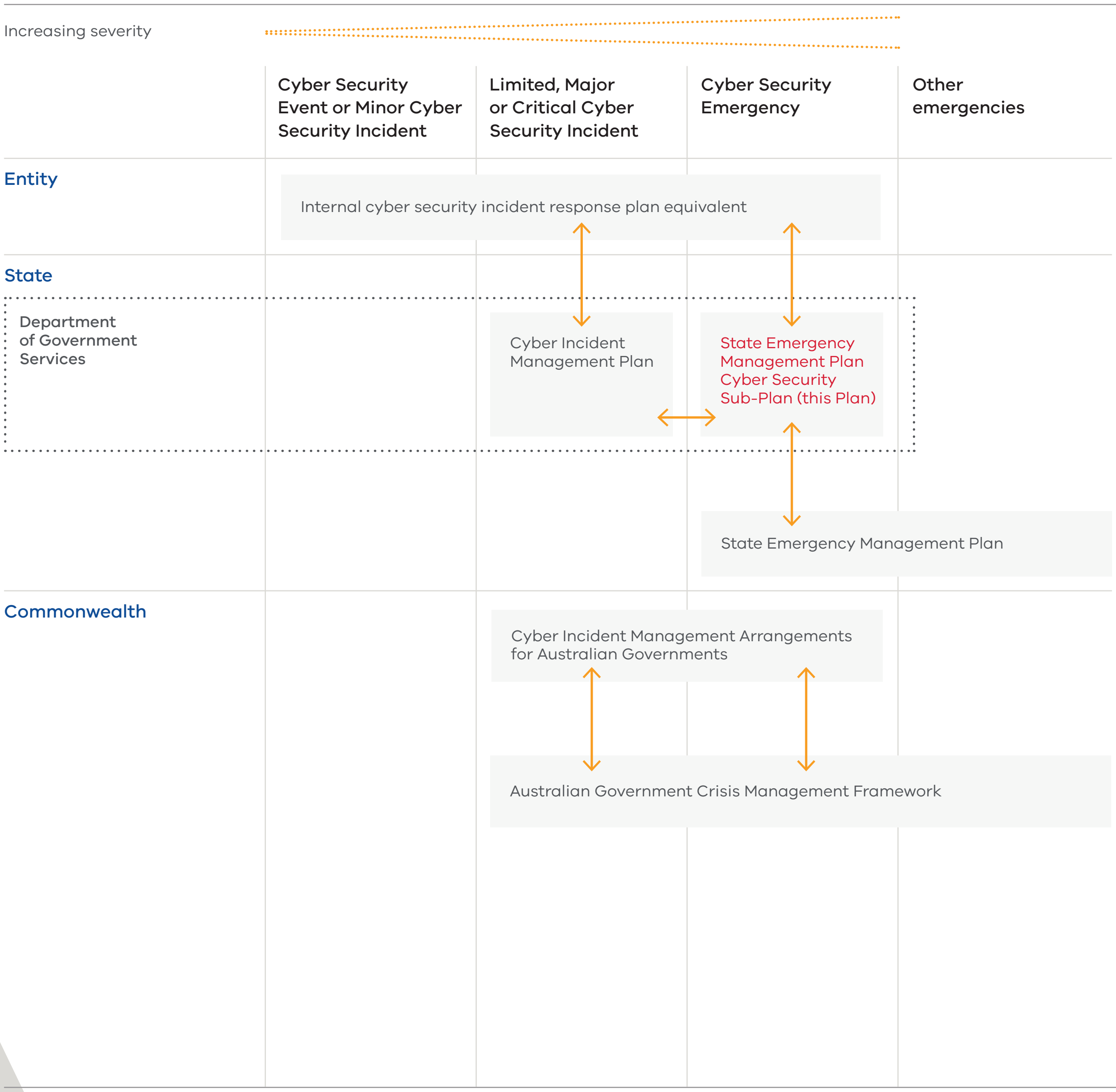
All other stakeholders beyond this Plan's authority are welcome to consider this Plan for their own purposes. This may include the development of their own arrangements or better understanding roles and responsibilities required in the event of compromise of cyber security. These other stakeholders may include, but are not limited to:

- the Commonwealth Government, including:
  - Australian Cyber Security Centre
  - Department of Home Affairs
  - National Emergency Management Agency
- the National Cyber Security Committee
- governments of other states and territories
- interested Victorian community members.

2.5 This Plan considered in the context of Victoria's cyber security management framework

The arrangements in this Plan align with Victorian and Commonwealth cyber security risk management arrangements.

TABLE 4: Victoria's cyber security event, incident and emergency management framework



Increasing severity	Cyber Security Event or Minor Cyber Security Incident	Limited, Major or Critical Cyber Security Incident	Cyber Security Emergency	Other emergencies
Entity	Internal cyber security incident response plan equivalent			
State				
Department of Government Services		Cyber Incident Management Plan	State Emergency Management Plan Cyber Security Sub-Plan (this Plan)	
			State Emergency Management Plan	
Commonwealth		Cyber Incident Management Arrangements for Australian Governments		
		Australian Government Crisis Management Framework		

Table continues next page.

Table of contents

Table continued from last page

Level	Arrangement	Issued by	Summary
Entity	Internal cyber security incident response plan equivalent	Entity	Refer to Table 3
State	Cyber Incident Management Plan	Department of Government Services	Refer to Table 3
	State Emergency Management Plan Cyber Security Sub-Plan (this Plan)	Department of Government Services on behalf of the Emergency Management Commissioner	Refer to Table 3
	Victoria State Emergency Management Plan	Emergency Management Commissioner	Outlines Victoria's arrangements for the mitigation of, preparedness for, response to and recovery from all major emergencies, and agency roles and responsibilities.
Commonwealth	Cyber Incident Management Arrangements for Australian Governments	National Cyber Security Committee	Aims to reduce the scope, impact and severity of national cyber security incidents on all Australians. The arrangements include principles and inter-jurisdictional coordination arrangements for Australian governments' cooperation in response to national cyber security incidents.
	Australian Government Crisis Management Framework	Department of Prime Minister and Cabinet	Outlines the Australian Government's approach to preparing for, responding to and recovering from crises. The Australian Government seeks to manage risks holistically using an 'all-hazards' approach that includes mitigating, planning and assisting states and territories, where appropriate, in managing emergencies resulting from a combination of natural and human-induced events. The framework provides ministers and senior officials with guidance on their respective roles and responsibilities. It also sets out the arrangements that link ministerial responsibility to the work of key officials, committees and facilities.

3 Introduction to cyber security arrangements

3.1 Defining 'cyber security emergency'

The Victorian Government defines a cyber security emergency as a serious or exceptional compromise of cyber security that must also include potential to cause or is causing:

- loss of life or serious injuries
- extensive damage to property, infrastructure or the environment
- significant adverse consequences for the Victorian community or a part of the Victorian community
- widespread disruption to, and/or damage or destruction of, critical infrastructure
- disruption to emergency service activities requiring re-prioritisation to meet expected levels of service
- large-scale economic consequences for Victoria.

A cyber security emergency is a Class 2 emergency under the *Emergency Management Act 2013 (Vic).*

Where a cyber security emergency involves, or is reasonably suspected to involve, an act of terrorism, it may be deemed a Class 3 emergency. Victoria Police is responsible for control and coordination for Class 3 emergencies in Victoria.

Appendix B expands on this list of common sources of cyber security compromise that are most likely to result in the consequences listed above:

- ransomware
- malware infections
- denial of service (DoS) and distributed denial of service (DDoS) attacks
- phishing and social engineering
- a data breach.

Table of contents

3.2 Cyber security as a state significant risk

The Victorian Government recognises 'cyber incidents' as a state significant risk.[5] This means there are potential consequences or impacts of the risk for the community, government and private industry that are material at the state level.

The assessment of cyber security as a state significant risk is corroborated by:

- Emergency Management Victoria's Victorian Emergency Risk Assessment, which sets Victoria's emergency risk profile
- the Sector Resilience Plans, which are prepared annually by the responsible departments for Victoria's 8 critical infrastructure sectors and supported by Sector Resilience Networks (**Appendix C**).

3.3 Guiding principles

Victoria's cyber security arrangements operate on an understanding that all departments and government agencies adopt the following guiding principles for cyber security incident management:

- use the State Emergency Management Plan's State Emergency Management Priorities (see **Appendix D**) to underpin and guide all decisions during the response to a cyber security emergency
- remain responsive to changes in the cyber security risk environment, including responding quickly to cyber security events, incidents and emergencies and their consequences
- remain accountable for protecting their own networks against cyber security threats, including the application of relevant regulatory controls
- collaborate with the Department of Government Services' Cyber Incident Response Service before, during and after cyber security emergencies, where relevant.

[5] The term 'cyber incidents' used in the state-level emergency risk assessment is considered interchangeable with the term 'cyber security incidents' used in this Plan.

D
Compare
Indicators
Templates
Alert
Ideas

4 Victoria's Cyber Defence Centre

The Department of Government Services, through the Victorian Government Cyber Defence Centre, leads Victoria's response to cyber security emergencies as Control Agency for cyber security emergencies under Victoria's emergency management arrangements.[6]

The Cyber Defence Centre operates 24/7, all-year-round to help departments, government agencies and councils to reduce the likelihood and impact of cyber security incidents and emergencies for Victorians.

The Cyber Defence Centre provides the following services:

- Victorian Government Security Operations Centre
- cyber incident response
- digital forensics
- threat monitoring and intelligence sharing
- social and news media monitoring
- a self-service portal
- vulnerability management.

In the event of a widescale cyber security emergency in Victoria that requires substantial technical resources, the Cyber Incident Response Service will prioritise its response in line with the State Emergency Management Priorities (**Attachment A**).

The Cyber Incident Response Service is available via 1300 278 842 (monitored 24/7) or cybersecurity@dpc.vic.gov.au[7] (monitored during business hours).

[6] Victorian State Emergency Management Plan.

[7] At the time of publication, the email address remains as cybersecurity@dpc.vic.gov.au. This is likely to be updated to cybersecurity@dgs.vic.gov.au before this plan is updated again.

5 Cyber security emergency mitigation

'Mitigation is the elimination or reduction of the incidence or severity of a compromise of cyber security, and the minimisation of its effects.'[8]

5.1 Threat intelligence

5.1.1 Summary

Cyber security threat intelligence products can be prepared in anticipation of, during or following a compromise of cyber security. Threat intelligence provides insights into issues, trends, likelihood and consequences, that require mitigation to reduce likelihood and harm. Threat intelligence products include:

- threat alert
- threat advisory
- threat intelligence brief
- threat intelligence summary
- incident situational report (SITREP).

A summary of these intelligence products and their common audience appears in **Appendix E**.

To ensure that information is shared with the correct audience, Victoria uses the Australian Cyber Security Centre's traffic light protocol when distributing all threat intelligence products. This protocol does not replace information management markers.

TABLE 5: Threat intelligence designations

Traffic light protocol	Definition
Red	Not for disclosure, restricted to recipients only
Amber + Strict	Limited disclosure, restricted to recipient's entity only
Amber	Limited disclosure, restricted to recipients' entity and its clients or contractors
Green	May be disseminated to recipients' stakeholders as deemed necessary
Clear	Disclosure is not limited

[8] Adapted from the Victorian State Emergency Management Plan.

Table of contents

5.1.2 Roles and responsibilities

5.1.2.1 Australian Cyber Security Centre

- Share threat intelligence with the Cyber Incident Response Service where a threat has potential or realised impact for Victorians.

5.1.2.2 Cyber Incident Response Service

- Receive and share threat intelligence. This includes:
  - gathering cyber security information and intelligence across a broad range of stakeholders (including, but not limited to other governments or private industry sources and analysis of cyber security incidents, risks and issues)
  - preparing and disseminating threat intelligence products, in anticipation of, or in response to an incident or threat (for example, a global trend that has not yet impacted Victoria).

5.1.2.3 All entities

- Act on relevant threat intelligence issued by the Cyber Incident Response Service.
- Analyse potential threats to determine whether a cyber security incident is occurring or has occurred and report any detections to the Cyber Incident Response Service.
- Share threat intelligence with relevant portfolio Sector Resilience Network Chair/s and/or contracted service providers, including managed service provider/s, in line with advised traffic light protocol and where appropriate.

5.1.2.4 Sector Resilience Network Chairs

- Provide the Sector Resilience Network membership (private industry and public sector critical infrastructure owners and operators) or key stakeholder groups with relevant threat intelligence provided by the Cyber Incident Response Service for awareness. Refer to **Appendix C** for more information on Sector Resilience Networks.

5.2 Improving cyber security maturity

5.2.1 Summary

Many cyber security compromises are traced back to a low level of cyber security maturity in one or more areas. Identifying and managing risks relating to the integrity and availability of digital systems, services and information is a compelling risk mitigation strategy. Strategies and remediation activities should reflect the risk held by the entity.

A summary of the frameworks referenced throughout the remainder of this sub-section appears in **Appendix F.**

5.2.2 Roles and responsibilities

5.2.2.5 Department of Home Affairs (Commonwealth)

- Lead the coordinated development and implementation of national cyber security policy for the Australian Government.
- Regulate cyber and critical infrastructure security, via the Department of Home Affairs' Cyber and Infrastructure Security Centre.

5.2.2.6 Department of Government Services

- Consider the implementation of the 2023–2030 Australian Cyber Security Strategy.

5.2.2.7 Departments and government agencies

- Adopt one or a combination of these two approaches, to the level that is appropriate for the risk of the entity:
  - Australian Cyber Security Centre's Essential Eight Maturity Model
  - The National Institute of Standards and Technology (USA) Cyber Security Framework.
- If full alignment with one or a combination of these approaches is not possible, departments and government agencies should consider their cyber security risk profile, or an agreed industry standard, to determine the appropriate level of maturity to apply.
- Implement the Victorian Protective Data Security Framework and Standards as per the Privacy and Data Protection Act 2014 or other relevant standards as required.
- As required, adopt these approaches:
  - apply the Protective Security Policy Framework and subsequently the Information Security Manual when holding and accessing Australian Government sensitive and security classified information
  - apply the Victorian Government Risk Management Framework.

- Where relevant, adopt these approaches:
  - energy sector: Australian Energy Sector Cyber Security Framework
  - agencies holding health information: implement a framework to protect the privacy of individuals' health information as per the *Health Records Act 2001*.
- Consider engaging contracted service providers which are Information Security Registered Assessors Program assessed with consideration to system classification or SOC II Type 2 accreditation, if that provider may support the response to a cyber security emergency with access to data that is Business Impact Level 3 or higher (see **Appendix I**).
- Engage contracted service providers with contracts that outline the requirement to cooperate with this Plan during cyber security emergencies.

5.2.2.8 Department of Government Services

- Provide advice to support a department, government agency or council to determine the appropriate level of cyber security maturity to apply on request.

5.3 Community and industry awareness and engagement

5.3.1 Summary

For community and industry[9] to effectively take responsibility for their own cyber security, they must receive timely, relevant and tailored support to assist in making informed decisions.

5.3.2 Roles and responsibilities

5.3.2.1 Department of Government Services

- Lead initiatives which foster a cyber resilient Victorian community and industry, aligned to the vision and objectives of Victoria's Cyber Strategy 2021.

[9] The reference to industry in this section is a reference to wider industry and is not intended as a specific reference to critical infrastructure owners and operators. Roles and responsibilities for critical infrastructure owners and operators are addressed elsewhere in this Plan.

6 Cyber security emergency preparedness (identify, protect and detect)

‘Preparedness includes the activities to prepare for and reduce the effects of a compromise of cyber security by having plans, capability and capacity for response and recovery.’[10]

6.1 Identify cyber security risk

6.1.1 Summary

> Develop maturity to manage cyber security risks to the confidentiality, integrity or availability of information, systems or services.

6.1.2 Roles and responsibilities

6.1.2.1 Departments and government agencies

- In line with the Office of the Victorian Information Commissioner’s Five Step Action Plan relating to information security, departments and government agencies should:
  - identify information assets.
  - determine the ‘value’ of this information.
  - identify any risks to this information.
  - apply security measures to protect the information.
  - manage risks across the information lifecycle.
- Identify and document critical processes, asset details, network topographies and key contacts.
- Maintain an inventory of hardware and software, including cloud-based applications and virtual infrastructure.
- Establish policies for cyber security that include roles and responsibilities.
- Identify threats, vulnerabilities, and risk to assets.
- Ensure playbooks and business continuity plans are developed if critical assets need to be taken offline.

[10] Adapted from the State Emergency Management Plan.

Table of contents

- Share information with the Victorian Government Chief Information Security Officer, on request.
- Comply with any relevant state or Commonwealth legislation or guidelines that relate to cyber security.

6.1.2.2 Department of Government Services

- Maintain Victoria's cyber security emergency management arrangements and its capability as Control Agency for cyber security emergencies.
- Educate stakeholders on the state's cyber security emergency management arrangements.
- Produce and share advice about new and emerging cyber security risks, including recommendations to mitigate these risks, in partnership with the Australian Government's Australian Cyber Security Centre and Department of Home Affairs, to support preparedness for government, industry and the community.

6.1.2.3 Victorian Government Chief Information Security Officer

- Request an entity to provide any information that may be necessary, for the purposes of being prepared for a cyber security emergency.

6.2 Protect from cyber security risk

6.2.1 Summary

> Entities are responsible for developing and implementing the appropriate safeguards to ensure the confidentiality, integrity or availability of information, systems or services.[11]

6.2.2 Roles and responsibilities

6.2.2.1 All entities

- Manage access to assets and information.
- Protect sensitive data.
- Conduct regular backups.
- Protect devices.
- Manage device vulnerabilities.
- Regularly train and retrain users of the department or agency's cyber security policies and procedures, as well as those specific to roles and responsibilities.
- Respond to requests from the Victorian Government Chief Information Security Officer, for the purposes of being prepared for a cyber security emergency.
- Review cyber insurance arrangements at least annually.
- Comply with any relevant state or Commonwealth legislation or guidelines that relate to cyber security and risk management.

[11] Modified from the NIST Framework

6.2.2.2 Department of Government Services

- Provide cyber security advice, guidance and central cyber security services, including through the Cyber Incident Response Service, to support departments, government agencies and councils protect against cyber security risk.

6.2.2.3 Contracted service providers

- Provide assurance to the entity that the management of the cyber risk/s is commensurate with the value of the information, system or service, in line with contractual responsibilities.

6.3 Maintain and exercise plans and arrangements

6.3.1 Summary

> Entities are responsible for preparing, reviewing, exercising and updating their own cyber security incident response plans and arrangements.

6.3.2 Roles and responsibilities

6.3.2.1 Cyber Incident Response Service

- In support of entities developing their own plans, maintain a cyber security incident response plan which aligns with the arrangements detailed in this Plan.
- With regard to available resources, determine and agree upon a suitable level of input and participation in department, government agency and council cyber security exercises when requested (for example, provide subject matter expertise to support the development and delivery of a desktop exercise).

6.3.2.2 Department of Government Services

- Conduct at least one exercise of this Plan annually.
- Review and update this Plan at least every 3 years, with consideration to the outcomes of annual exercises.
- Educate stakeholders on the state's cyber security arrangements.

6.3.2.3 Secretary, Department of Government Services (Control Agency Officer in Charge)

- Maintain a list of persons authorised to perform the role of Class 2 State Controller – Cyber Security and advise the Emergency Management Commissioner of any changes to this list.

6.3.2.4 All entities

Prepare and implement a cyber security incident response plan that:[12]

- addresses the mitigation of, preparedness for, response to and recovery from a cyber security compromise, including roles and responsibilities:
  - is consistent with this Plan and the Cyber Incident Management Plan
  - is in line with Victorian Protective Data Security Standards, specifically, Standard 6 – establish, implement and maintain an information security incident management process relevant to size, resources and risk posture.

- In line with the cyber security incident response plan:
  - educate executive and senior management, including the role of executive and senior management during a cyber security event, incident or emergency
  - assess internal capability and capacity for the identified roles and responsibilities, and prepare a plan to address any identified gaps
  - create and regularly review incident response processes and procedures
  - conduct an annual exercise.

- Exercises may take the form of an internal discussion exercise, ranging up to a multi-agency deployment-style exercise[13]. Exercises may consider engaging:
  - both cyber and emergency management personnel
  - multi-agency stakeholders (such as critical infrastructure or other departments)
  - relevant community or community organisations
  - pursue any areas for improvement identified through this exercise.

6.4 Detection

6.4.1 Summary

There is no single process for detecting a compromise of cyber security. Detection often involves:

Precursors, such as:

- identifying that a cyber security compromise might occur in the future, such as the receipt of a threatening email or news of a global malware/ ransomware attack (note: this form of detection is rare).

Indicators, such as:

- detection that a cyber security compromise may have occurred (e.g. intrusion detection alerts, file names with odd characters, configuration changes)
- reports of unusual or suspicious activity by staff or external stakeholders
- systems or services not operating or functioning as expected
- unusual activity.

[12] Optional template available at Cyber Incident Response Plan template.

[13] ACSC has prepared 'Exercise in a Box' scenario resources that may be helpful when undertaking the exercise.

Security monitoring, such as:

- referral from a managed security service provider or another organisation/stakeholder, alerting to the presence of a cyber security compromise.

Appendix G identifies steps that are useful in confirming the presence of a cyber security compromise.

6.5 Roles and responsibilities

6.5.1 Cyber Incident Response Service

- Lead the monitoring of cyber security threats affecting Victoria's assets, in close consultation with the Australian Cyber Security Centre.

6.5.2 Entity

- Consider potential threats, paying attention to common indicators.

7 Cyber security emergency response

‘Response is the action taken immediately before, during and in the first period after a compromise of cyber security to reduce the effects and consequences of the incident.’[14]

7.1 Analysis

7.1.1 Summary

It is important to consider all indicators of a cyber security compromise to confirm in a timely manner whether a compromise has occurred, or is occurring. Incident analysis can continue simultaneously with other processes, such as incident notification.

7.1.2 Roles and responsibilities

7.1.2.1 Entity with compromised cyber security

- Determine scope, impact and severity.
- Commence incident notifications.
- Collect and record evidence.[15] For example:
  - hard drive images and raw images, RAM images
  - IP addresses
  - network packet captures and flows
  - network diagrams
  - log and configuration files[16]
  - databases
  - incident response and investigation notes
  - screenshots
  - social media posts
  - CCTV, video and audio recordings
  - documents detailing the monetary cost of remediation or loss of business activity.

[14] Adapted from the State Emergency Management Plan.

[15] The Victorian Managed Insurance Authority or other cyber insurance provider will normally require this evidence.

[16] Refer to the Victorian Government Log Collection and Retention Guidelines, available from the Department of Government Services.

- Collate, record and securely store all evidence that is collected.
- Create and maintain a log of all evidence collected. This should detail the date and time evidence was collected, who it was collected by, and details of each item collected.
- Ensure all access to evidence is recorded in the evidence log, including the rationale for access. This is important in maintaining the 'chain of custody' for collected evidence.
- Minimise the frequency evidence is transferred between staff, and record details of any such transfer.

7.2 Notification

7.2.1 Summary

> Different entities have different responsibilities for notifying key stakeholders about events, incidents and emergencies. After confirming whether a cyber security compromise has occurred, or continues to occur, notification should commence as quickly as practicable.
>
> Notification is not required if the cyber security incident is considered by the entity to be a minor cyber security incident or cyber security event.
>
> Contact details for key stakeholders are included at **Appendix H**.

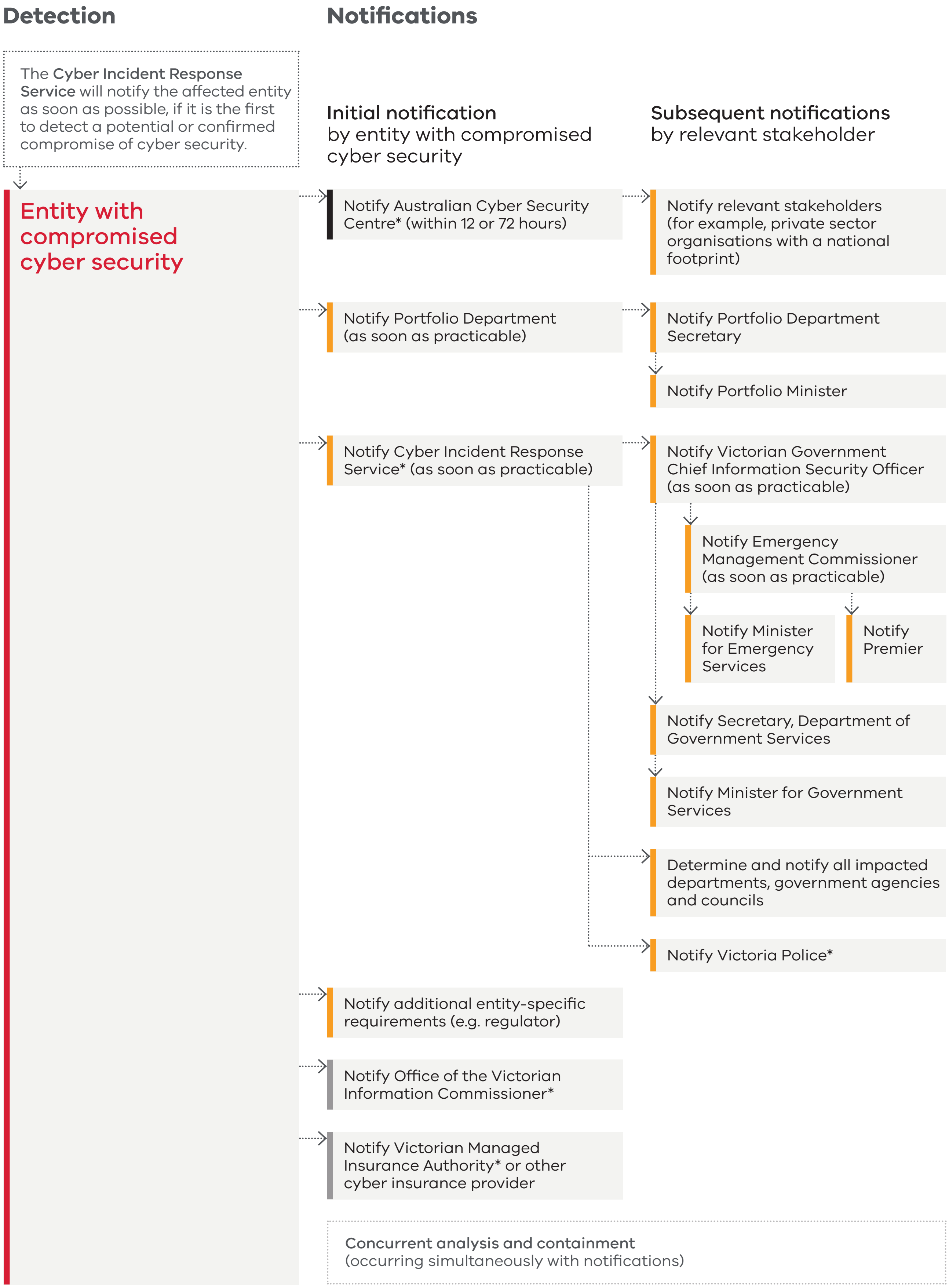
7.2.2 Roles and responsibilities

The entity that detects the cyber security compromise is responsible for ensuring timely initial notification is made to relevant stakeholders.

The entity notifying of an incident must provide the same or similar information to several stakeholders. For example, a public sector critical infrastructure owner or operator will be required to notify the Australian Cyber Security Centre, Department of Government Services' Cyber Incident Response Service and relevant portfolio department.

Acknowledging there is a duplication in the notification process, the entity is welcome to engage the Cyber Incident Response Service's assistance to help streamline notifications on a case-by-case basis.

FIGURE 3: Notification responsibilities



Detection

The **Cyber Incident Response Service** will notify the affected entity as soon as possible, if it is the first to detect a potential or confirmed compromise of cyber security.

Entity with compromised cyber security

Notifications

Initial notification by entity with compromised cyber security

Notify Australian Cyber Security Centre* (within 12 or 72 hours)

Notify Portfolio Department (as soon as practicable)

Notify Cyber Incident Response Service* (as soon as practicable)

Notify additional entity-specific requirements (e.g. regulator)

Notify Office of the Victorian Information Commissioner*

Notify Victorian Managed Insurance Authority* or other cyber insurance provider

Subsequent notifications by relevant stakeholder

Notify relevant stakeholders (for example, private sector organisations with a national footprint)

Notify Portfolio Department Secretary

Notify Portfolio Minister

Notify Victorian Government Chief Information Security Officer (as soon as practicable)

Notify Emergency Management Commissioner (as soon as practicable)

Notify Minister for Emergency Services

Notify Premier

Notify Secretary, Department of Government Services

Notify Minister for Government Services

Determine and notify all impacted departments, government agencies and councils

Notify Victoria Police*

Concurrent analysis and containment (occurring simultaneously with notifications)

● Required notification for all entities

● Required notification for critical infrastructure owners or operators (as determined by the *Security of Critical Infrastructure Act 2018*)

● Required notification for department, government agency, council and contracted service providers

∗ Additional comments on page 28

Notes for Figure 3

Australian Cyber Security Centre

As per the *Security of Critical Infrastructure Act 2018*, critical infrastructure owners and operators (as determined under the Commonwealth's Security of Critical Infrastructure arrangements) must notify the Australian Cyber Security Centre within 12 hours if the incident has had or is having a significant impact on the availability of an asset[17], or 72 hours if the incident has had, is having, or is likely to have, a 'relevant impact' on an asset[18].

Cyber Incident Response Service

Any report made to the Australian Cyber Security Centre will be forwarded to the Department of Home Affairs, as the critical infrastructure security regulator.

The report to the Australian Cyber Security Centre will not be forwarded to the Victorian Government.

To ensure Victoria can respond to potential consequences to the Victorian community, this plan outlines an additional reporting process to the Cyber Incident Response Service, separately. While private industry critical infrastructure owners and operators are outside of the key audience of this plan, they should align with this requirement to notify the Cyber Incident Response Service and key operational stakeholders of the relevant portfolio if there are supply impacts due to a cyber security emergency (including the Australian Cyber Security Centre where required by the *Security of Critical Infrastructure Act 2018*).

Victorian Protective Data Security Standards

Organisations that are subject to the Victorian Protective Data Security Standards must notify the Office of the Victorian Information Commissioner within 30 days if the incident compromises the confidentiality, integrity or availability of public sector information.

This is a requirement at Business Impact Level 2, as per the Victorian Protective Data Security Framework.

Victorian Managed Insurance Agency

The Victorian Managed Insurance Agency or other cyber insurance provider should be notified as soon as possible and be included in response and recovery. An impacted entity should liaise with their insurer before proceeding to incur significant costs for response and/or notification.

Victoria Police

Notifications to Victoria Police are required for any cyber security incident or emergency that is a suspected crime.

[17] A significant impact is one where both the critical infrastructure asset is used in connection with the provision of essential goods and services; and the incident has materially disrupted the availability of the essential goods or services delivered by a critical infrastructure asset or any of the circumstances specified in the rules exist in relation to the incident: *Security of Critical Infrastructure Act 2018* s30BEA.

[18] A relevant impact is an impact of the hazard on the availability, integrity, reliability, or confidentiality of your asset: *Security of Critical Infrastructure Act 2018* s8G.

7.3 Classification

7.3.1 Summary

The Victorian Government uses a 6-tier model for categorising cyber security incidents, of which the sixth category is a cyber security emergency (Table 1). Cyber security incidents are categorised based on the nature of the compromise and the impacts they create.

Appendix I identifies how these categories are prepared as a comparable state-level equivalent to the Office of the Victorian Information Commissioner's entity-level Business Impact Levels.

Cyber security emergencies are most likely to originate in government or larger businesses, particularly critical infrastructure owners and operators, where the disruption of services could threaten life or property or have significant adverse consequences for the Victorian community.

7.3.2 Roles and responsibilities

7.3.2.1 Secretary, Department of Government Services (Control Agency Officer in Charge)

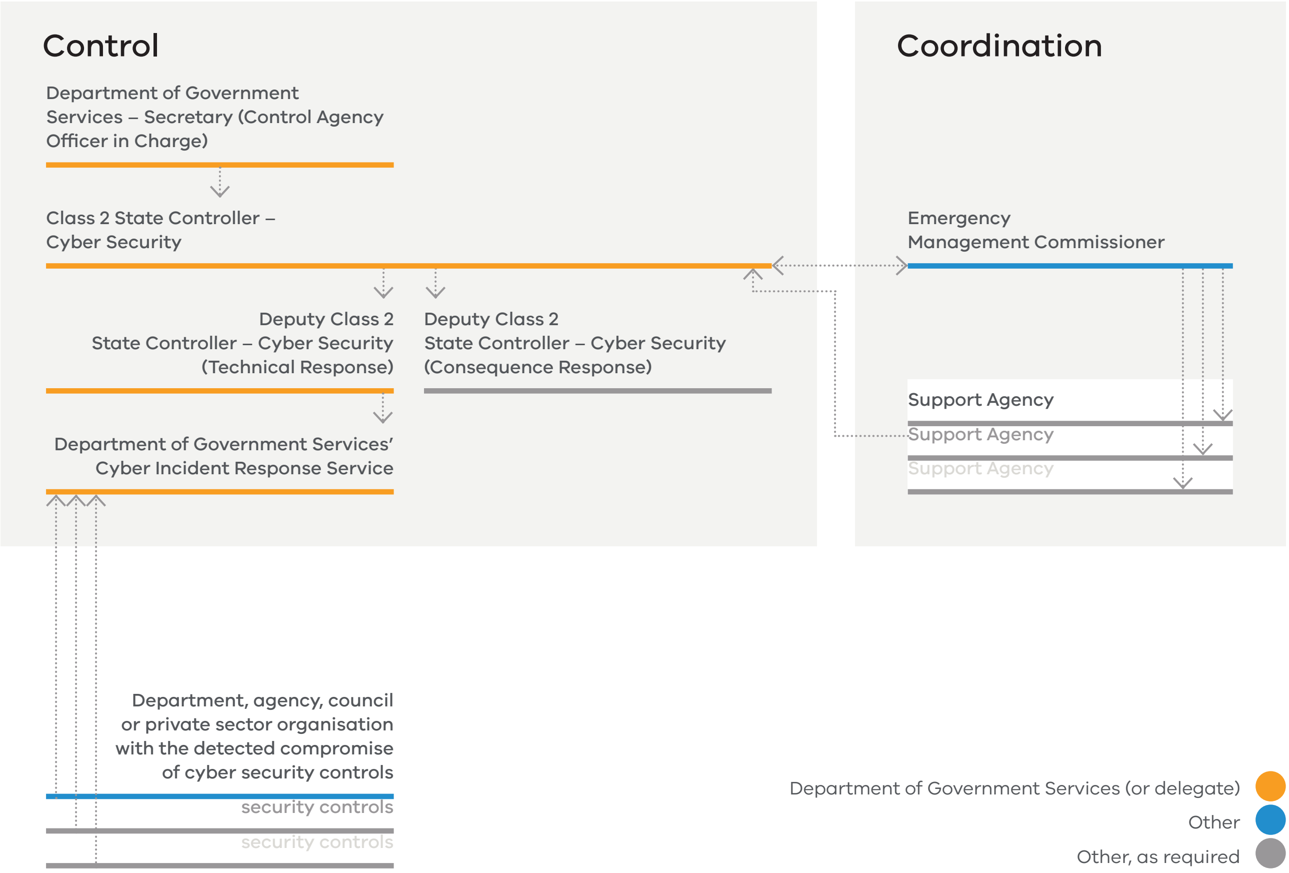
- Declare the occurrence of a cyber security emergency:
  - with consideration to the common characteristics of a cyber security emergency (refer to Table 1)
  - in consultation with the Emergency Management Commissioner
  - where relevant, with advice from the:
    - impacted entity
    - relevant portfolio government department
    - about whether it is necessary to activate Victoria's emergency management arrangements to ensure effective management of the situation.

7.4 Control

7.4.1 Summary

> Control is the direction of response activities across entities, horizontally, including the coordination and tasking of other agencies.

FIGURE 4: Control


Control
Department of Government Services – Secretary (Control Agency Officer in Charge)
Class 2 State Controller – Cyber Security
Deputy Class 2 State Controller – Cyber Security (Technical Response)
Deputy Class 2 State Controller – Cyber Security (Consequence Response)
Department of Government Services' Cyber Incident Response Service
Department, agency, council or private sector organisation with the detected compromise of cyber security controls
security controls
security controls
Coordination
Emergency Management Commissioner
Support Agency
Support Agency
Support Agency
Department of Government Services (or delegate)
Other
Other, as required

7.4.2 Roles and responsibilities

7.4.2.1 Emergency Management Commissioner

- Ensure that the response and recovery is coordinated and control arrangements are in place.
- Ensure that relevant agencies act in accordance with the State Emergency Management Plan.

7.4.2.2 Secretary, Department of Government Services (Control Agency Officer in Charge)

- Maintain overall control of response activities in relation to a Class 2 emergency. In practice, this includes ensuring control arrangements are effective and providing regular updates to the Emergency Management Commissioner on the suitability of these arrangements.
- Advise the Emergency Management Commissioner of the appointment of Class 2 State Controller/s – Cyber Security for the declared cyber security emergency, including the date of their appointment, with consideration to the prepared list of authorised people to perform the role of Class 2 State Controller – Cyber Security.

7.4.2.3 Class 2 State Controller – Cyber Security

- Responsible for control of the emergency.
- Chair the Class 2 State Control Team – Cyber Security.
- Be accountable and responsible for activities delegated to any Deputy Class 2 State Controller, and all the functions of incident management (as per the Australasian Inter-Service Incident Management System; see **Appendix J**).
- Appoint a Deputy Class 2 State Controller – Technical Response.
- If required, appoint Deputy Class 2 State Controller/s – Cyber Security (Consequence Response), to support the Emergency Management Commissioner role in consequence management. Multiple Deputy Class 2 State Controller/s – Cyber Security (Consequence Response) may be appointed to address different consequences.
- Develop a Whole of Victorian Government picture of the emergency.
- Develop a Whole of Victorian Government Incident Action Plan, in consultation with the Emergency Management Commissioner.
- Request support from the following as support agencies:
  - relevant Victorian departments, government agencies[19]
  - Commonwealth-level departments or agencies, including the Australian Cyber Security Centre.

7.4.2.4 Deputy Class 2 State Controller – Cyber Security (Technical Response)

- Develop and implement an action plan relating to overseeing the technical response, including containment and eradication.

7.4.2.5 Cyber Incident Response Service

- Provide direct support to the Deputy Class 2 State Controller – Cyber Security (Technical Response)

[19] As per Table 10: Support agencies for response, from the State Emergency Management Plan.

7.4.2.6 Deputy Class 2 State Controller/s – Cyber Security (Consequence Response)

- Develop and implement an action plan relating to the consequence/s assigned to the Deputy Class 2 State Controller/s – Cyber Security (Consequence Response).

7.4.2.7 Department of Government Services

The Department of Government Services is the control agency for cyber security emergencies in Victoria.[20] This means that the Department of Government Services is:

- primarily responsible for managing the response to a cyber security emergency
- responsible for establishing the management arrangements for an integrated response to a cyber security emergency.

7.4.2.8 Entity with compromised cyber security

- Appoint an Entity Incident Manager.

7.4.2.9 Entity Incident Manager

- Develop a Technical Response Incident Action Plan.
- Perform all functions of incident management within the department or government agency (as per the Australasian Inter-Service Incident Management System; see **Appendix J**).
- Activate an internal Incident Management Team to delegate particular functions to as required, to resolve the incident using local resources. The Incident Management Team may respond from a dedicated operations room.
- Seek Cyber Incident Response Service assistance if additional resources are required.

7.5 Class 2 State Control Team – Cyber Security

7.5.1 Summary

The Class 2 State Control Team – Cyber Security will implement the strategic context for response (readiness, control and relief) and for the integration of relief and recovery, which includes:

- supporting control functions and responsibilities on behalf of the Emergency Management Commissioner
- implementing the strategic context of operational readiness for, response to and where appropriate the integration of, relief and recovery.

[20] As per Table 9: Control agencies for response, from the State Emergency Management Plan.

7.5.2 Roles and responsibilities

For a cyber security emergency, the Class 2 State Control Team – Cyber Security membership is:

- Class 2 State Controller – Cyber Security (Chair)
- Emergency Management Commissioner
- a senior member of the entity with compromised cyber security
- a senior member of each key support agency
- others as determined by the Emergency Management Commissioner and Class 2 State Controller – Cyber Security.

Note: Consideration should be given to the mixture of emergency management and cyber security expertise that is represented on the team.

7.6 Transfer of control where there are significant consequences

7.6.1 Summary

> While the Department of Government Services is the Control Agency for cyber security emergencies, there may be situations where another department or government agency is best placed to become the Control Agency, based on the nature and extent of consequences associated with the emergency.
>
> The transfer of Control Agency responsibilities will be managed in accordance with the arrangements detailed in the State Emergency Management Plan.
>
> This section relates to the transfer of control of another emergency with consequences that are directly related to a cyber security emergency. How to manage a concurrent cyber security emergency and other Class 1 (such as fire) or Class 2 emergency (such an earthquake) is covered in a later section.

7.6.2 Roles and responsibilities

7.6.2.1 Emergency Management Commissioner

- Ensure control arrangements are in place before and after a transfer of control.
- Consult with the relevant Control Agency to consult prior to transferring control to another agency, so that the Control Agency can provide assurance to the Emergency Management Commissioner that control arrangements will remain in place after the transfer.

7.6.2.2 Department of Government Services, if not determined the Control Agency

- Assume the role of a support agency responsible for leading the technical response to the emergency, if required.
- Provide staffing to fill the Deputy Class 2 State Controller – Cyber Security (Technical Response) roster, if requested.

7.6.2.3 Department or government agency that the Control Agency responsibility is transferred to (the receiving department or government agency)

- Jointly agree with the Emergency Management Commissioner and Department of Government Services the appropriate emergency management arrangements and structure, with regard to this Plan.
- Continue to collaborate with the Emergency Management Commissioner and Department of Government Services for the duration of any cyber security components of the emergency.
- In any instance where the receiving department or government agency is already the Control Agency for a separate emergency that has been declared due to a significant consequence of the cyber security emergency (for example, a health emergency), the receiving department or government agency will, in consultation with the Emergency Management Commissioner and Department of Government Services, agree whether to continue the two separate emergencies in parallel or to combine the two declared emergencies into one. If the cyber security emergency declaration is discontinued, the arrangements relevant to the other declared emergency will prevail.

7.7 Transfer of control where the cyber security emergency is a suspected criminal act

7.7.1 Summary

If a cyber security emergency is reasonably believed to be the result of a serious criminal act, including elements of a siege, hijack or terrorism, the emergency may be better classified as a Class 3 emergency and where Victoria Police assume the role of Control Agency.

The transfer of Control Agency responsibilities will be managed in accordance with the arrangements detailed in the State Emergency Management Plan. Where the Department of Government Services transfers control to another department or government agency, it will assume the role of a support agency responsible for leading the technical response to the emergency, if required.

7.7.2 Roles and responsibilities

7.7.2.1 Emergency Management Commissioner

- Ensure effective control arrangements are in place for a Class 2 Major Emergency.

7.7.2.2 Chief Commissioner of Police

- Ensure control arrangements are in place where the event is transferred to Victoria Police on the basis that it is a Class 3 emergency. In the case that the event becomes a Class 3 emergency, Victoria Police becomes the Control Agency and the emergency response transitions to the Class 3 arrangements as per the State Emergency Management Plan Class 3 Sub-Plan.

7.7.2.3 Relevant Control Agency

- Consult with the Emergency Management Commissioner and the Chief Commissioner of Police prior to transferring control to Victoria Police.

7.8 Control centre

7.8.1 Summary

A cyber security emergency will likely require response from a wide range of representatives from beyond the Department of Government Services. While many may be able to continue working from their business-as-usual locations, the Department of Government Services may decide to activate and work from Victoria's State Control Centre, or another location.

7.8.2 Roles and responsibilities

7.8.2.1 Secretary, Department of Government Services (Control Agency Officer in Charge)

- Determine the location where the emergency is controlled from in consultation with the Class 2 State Response Controller – Cyber Security.
- Consult with the Emergency Management Commissioner if seeking to control the emergency from Victoria's State Control Centre.

7.9 Controlling Victorian consequences of a national cyber security incident or emergency

7.9.1 Summary

In the event of a cyber security emergency with national implications, the Department of Government Services and the Victorian Government will remain responsible for the management of the emergency in Victoria.

7.9.2 Roles and responsibilities

7.9.2.1 Australian Cyber Security Centre

- If a cyber security emergency impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or requires a coordinated inter-jurisdictional response, the Australian Cyber Security Centre may declare a national cyber incident. This declaration will occur in consultation with cyber security leaders from affected state and territory governments, via the National Cyber Security Committee.

7.9.2.2 Victorian Government Chief Information Security Officer

- Determine the categorisation and activation of Victorian arrangements to a national incident with consideration of the impact on Victorians.
- Act as Victoria's representative to the National Cyber Security Committee during a national cyber security incident.

7.9.2.3 National Cyber Security Committee

The National Cyber Security Committee comprises government cyber security leaders from all Australian federal, state and territory governments. It is responsible for supporting national coordination and increased situational awareness during national cyber security incidents.

On declaring a national cyber security incident, the National Cyber Security Committee will activate to support the national collaboration and coordination of response efforts. This includes:

- facilitating the exchange of threat intelligence and solutions to enhance jurisdictions' situational awareness and response activities.
- overseeing the development of nationally consistent public information
- providing a forum for consultation that informs members' briefings to their respective senior stakeholders (including Ministers).
- facilitating the sharing of expertise and resources to support jurisdictions' responses.

7.9.2.4 National Office of Cyber Security (Department of Home Affairs)

- The National Office of Cyber Security within the Australian Department of Home Affairs works to support Australia's resilience to, and recovery from, major cyber incidents.

  The National Cyber Security Coordinator ensures a coordinated approach to prepare for and manage the consequences of cyber security incidents by bringing together expertise and resources from across government and security agencies.

7.9.2.5 Department of Government Services

- The National Cyber Security Committee's Cyber Incident Management Arrangements for Australian Governments exist to support the Department of Government Services and the Victorian Government in coordinating response activity with other jurisdictions.

  Where state or Commonwealth coordination arrangements exist for specific industries or sectors, such as the national energy sector cyber security arrangements, the Department of Government Services will collaborate with the relevant bodies (including portfolio Victorian Government departments) to support an integrated operational response.

  Where a cyber security emergency has national implications, or impacts multiple states/territories simultaneously, the Department of Government Services will work closely with the Commonwealth Government, the Australian Cyber Security Centre, Victoria Police and emergency management agencies to determine the Victorian impacts and consequences of a national cyber security emergency, in accordance with the intention of this Plan.

  The Department of Government Services and the Victorian Government will remain responsible for operational management of any cyber security emergency within Victoria.

7.10 Managing a cyber security emergency with other concurrent Class 1 or 2 emergency/ies

7.10.1 Summary

The State Emergency Management Priorities (see **Appendix C**) underpin and guide all control and coordination decisions, including in the occurrence of:

- a cyber security emergency and a concurrent Class 1 or 2 emergency
- two separate cyber security emergencies
- a cyber security emergency and non-emergency cyber security incident/s.
- The State Emergency Management Priorities apply to all aspects of this Plan.

7.10.2 Roles and responsibilities

7.10.2.1 Emergency Management Commissioner

- Work with relevant Control Agencies to prioritise response roles according to the State Emergency Management Priorities.

7.10.2.2 Cyber Incident Response Service

- Work with relevant departments or agencies to prioritise the Cyber Incident Response Service's contribution to the response to each cyber security incident/ emergency, according to the State Emergency Management Priorities. Where prioritisation of a Cyber Incident Response Service resource is required, the Cyber Incident Response Service will implement a scaled response model, with priority given to a cyber security emergency, then cyber security incidents in descending order of their current or projected consequences.

7.10.2.3 Departments, government agencies and councils

- Where the Cyber Incident Response Service has implemented a scaled response model, source any additional response capacity required to respond to the relevant incident.
- Liaise with the Victorian Managed Insurance Authority or other cyber insurance provider to determine if additional capacity is available under a relevant insurance policy.

7.11 Coordination and ongoing engagement

7.11.1 Summary

> Coordination is the bringing together of people, resources, governance, systems and processes to ensure effective response and recovery.
>
> Effective coordination of a response requires opportunities for two-way communication between impacted stakeholders. As a general rule, communication should continue by and with each of the stakeholders involved with the initial notification of the incident, at a frequency and level of detail that allows each stakeholder to acquit their own areas of responsibility.

7.11.2 Roles and responsibilities

7.11.2.1 Emergency Management Commissioner

- Coordinate the activities of departments or agencies having roles or responsibilities to respond to the emergency.
- Identify and engage early with departments and government agencies with potential consequences, in consultation with the Class 2 State Controller – Cyber Security.

7.11.2.2 Class 2 State Controller – Cyber Security

- In consultation with appointed Deputy Controllers, prepare and circulate communications (including SITREPs) to support development of briefings to:
  - Victorian Government Chief Information Security Officer
  - relevant portfolio department/s and their respective minister/s
  - Emergency Management Commissioner
  - the Premier
  - Minister for Government Services
  - Minister for Emergency Services
  - impacted departments and government agencies
  - impacted private industry entity/ies.

7.11.2.3 Deputy Class 2 State Controller – Cyber Security (Technical Response)

- In consultation with the Cyber Incident Response Service, provide regular technical updates (including threat intelligence indicators of compromise) and general communications (such as SITREPs) to:
  - Class 2 State Controller – Cyber Security
  - Victorian Government Chief Information Security Officer
  - Chief Information Security Officers and Entity Incident Managers of:
  - impacted Victorian Government departments and government agencies.
  - all other potentially relevant Victorian Government departments and government agencies, to enable proactive action to protect themselves from potential impact
  - impacted private industry entity/ies.

7.11.2.4 Deputy Class 2 State Controller – Cyber Security (Consequence Response)

- In consultation with the relevant portfolio department or government agency, provide regular consequence updates and general communications (such as SITREPs) to:
  - Class 2 State Controller – Cyber Security
  - Emergency managers of:
    - impacted Victorian Government departments and government agencies.
    - all other potentially relevant Victorian Government departments and government agencies, to enable proactive action to protect themselves from potential impact
    - impacted private industry entity/ies.

7.11.2.5 Departments and government agencies

- Assist as a support agency, if requested, in line with Table 10 of the State Emergency Management Plan, and/or portfolio responsibilities. This may include performing a specific response (including relief) activity, or to ensure the continuity of its normal services or functions during a major emergency as part of managing a consequence. For example, this could include central agency advice and coordination functions.
- Liaise with private industry and relevant stakeholders, if requested.

7.11.2.6 Cyber Incident Response Service

- As required, engage with:
  - Australian Cyber Security Centre
  - Critical Infrastructure Sector Resilience Networks, via the Critical Infrastructure Resilience Sectors Forum
  - Law Enforcement Agencies
  - National Cyber Security Committee
  - Office of the Victorian Information Commissioner.

7.12 Media and public communication

7.12.1 Summary

The community needs information to make informed choices about their safety and to take responsibility for their own recovery. One of the State Emergency Management Priorities is the 'issuing of community information and community warnings detailing incident information that is timely, relevant and tailored to assist community members make informed decisions about their safety' (**Appendix C**).

Media and public communication should, where appropriate, provide information about:

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

The nominated spokesperson for communication during a cyber security emergency will vary depending on the circumstances of the emergency, its consequences and existing media comment or other concurrent incidents or emergencies (cyber security or other). Potential spokespeople should be one per aspect of the emergency, and include, but are not limited to:

- Victorian Premier or relevant minister
- Minister for Government Services
- Emergency Management Commissioner
- Class 2 State Controller – Cyber Security
- Victorian Government Chief Information Security Officer
- National Cyber Security Coordinator
- Government spokesperson with knowledge of the consequences of the emergency and relief and recovery arrangements.

7.12.2 Roles and responsibilities

7.12.2.1 Class 2 State Controller – Cyber Security

- Authorise all public communication in conjunction with the Victorian Government Chief Information Security Officer and Department of Government Services Chief Communications Officer or delegates.
- Activate the State Control Centre Public Information Officer and team where access to VicEmergency channels is considered advantageous.
- Issue warnings and information to the community in relation to the emergency, if regional controllers or incident controllers can't do so promptly, in consultation with the Emergency Management Commissioner and supported by the Department of Government Services communications team.
- Ensure the relevant minister is notified and provided with timely and up-to-date information in relation to the emergency, supported by the Department of Government Services communications team.

7.12.2.2 Emergency Management Joint Public Information Committee

- Support the Emergency Management Commissioner to develop appropriate communication and engagement plans.
- Coordinate media and public communication with the Department of Government Services, Emergency Management Commissioner and other departments and government agencies.

7.12.2.3 Cyber Incident Response Service

- Liaise with the Australian Cyber Security Centre and members of the National Cyber Security Committee (via the Cyber Incident Response Service manager's membership on the National Operations Sub-Committee) to share key messages about cyber security incidents to support consistent media and public communication across jurisdictions.
- Provide guidance to the State Control Centre Public Information Officer.

7.12.2.4 Department and government agencies

- Liaise and coordinate with the Emergency Management Joint Public Information Committee and Department of Government Services communications and media team to develop media and public communication.
- Liaise with the State Control Centre Public Information Officer to coordinate public communication activities.
- If the incident involves unauthorised access to or loss of personal information, and there is a risk of harm to the people the information is about, assess the risk of harm and consider notifying the affected people to minimise harm.[21]
- Manage own media and public communication channels (noting responsibility to liaise with the Emergency Management Joint Public Information Committee and State Control Centre Public Information Officer to coordinate media and public communication activities).

7.12.2.5 Entity with compromised cyber security

- Consult with the Victorian Managed Insurance Authority or other cyber insurance provider on communication. This is important as an admission of liability to the compromised cyber security can prejudice an insurance claim.

[21] Refer to the Office of the Victorian Information Commissioner's guide to Managing the Privacy Impacts of a Data Breach.

7.13 Technical response, including containment and eradication

7.13.1 Summary

In a cyber security incident, the technical response is of utmost importance as it is the only action that can address the root cause of the incident.

Appendix B provides a list of common cyber security incident types, along with the corresponding response activities which form the typical minimum response to minimise potential harm.

7.13.2 Roles and responsibilities

7.13.2.1 Deputy Class 2 State Controller – Cyber Security (Technical Response)

- Oversee the technical response, including containment and eradication.
- Work with the Entity Incident Manager to develop and oversee the effective implementation of its own internal Technical Response Incident Action Plan.
- Oversee the Cyber Incident Response Service response.
- Request support from the following as support agencies[22]:
  - relevant Victorian departments, government agencies
  - Commonwealth-level departments or agencies, including the Australian Cyber Security Centre
  - private industry cyber security experts (for example, expert technical advice or forensic services).

7.13.2.2 Cyber Incident Response Service

- Connect the department, government agency or council with the compromised cyber security with expert people, tools, services and knowledge to assist in effective analysis containment and eradication of cyber security threats.
- Develop and implement a Technical Response Incident Action Plan detailing containment, eradication and recovery activities.

7.13.2.3 Entity with compromised cyber security

- Undertake any technical activities necessary to respond to the incident.
- Collect and record technical evidence to support detailed forensic investigations, including law enforcement efforts to identify and prosecute potential cyber-attackers (**Appendix F**)
- Develop and implement a Technical Response Incident Action Plan detailing containment, eradication and recovery activities.
- Maintain an incident log.
- Seek Cyber Incident Response Service assistance if additional resources are required.

[22] Refer to the Office of the Victorian Information Commissioner's guide to Managing the Privacy Impacts of a Data Breach.

7.14 Consequence management

7.14.1 Summary

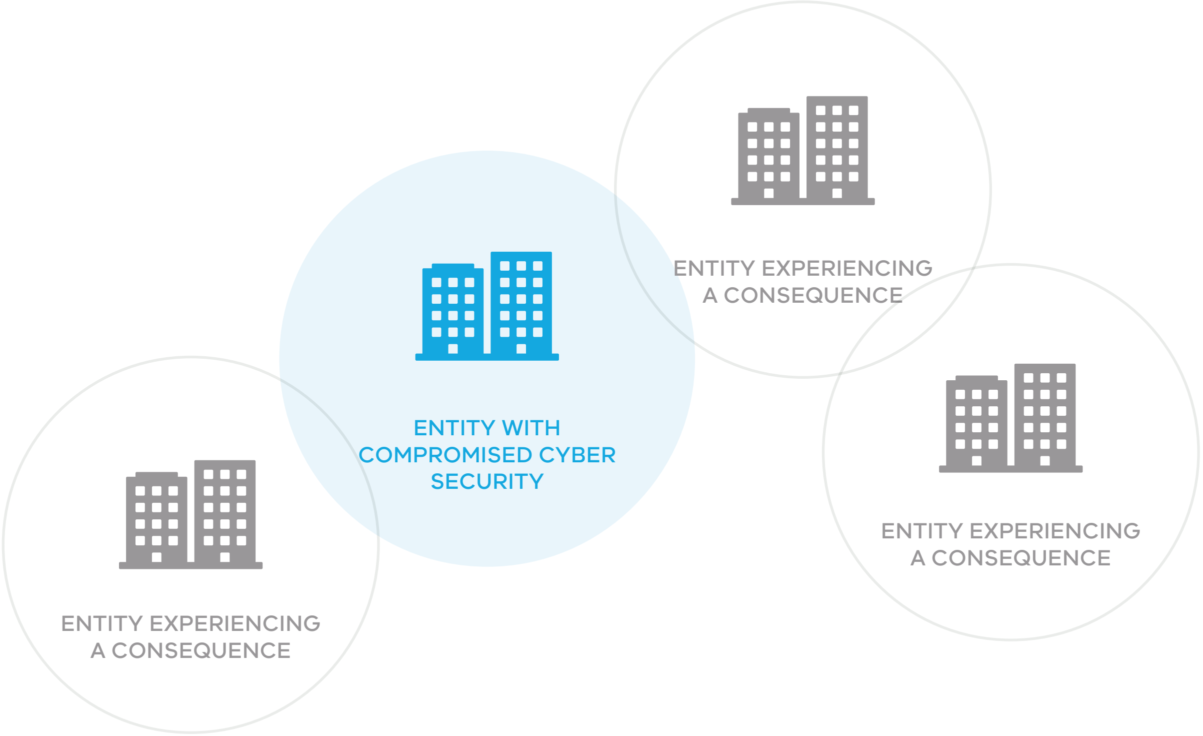
Consequence management relates to the second and subsequent order effects from cyber security incidents.

Victoria categorises cyber security incidents with consideration of an incident's consequences, both technical and non-technical (Table 1).

Consequence management occurs through the consideration of the wider ramifications of a cyber security compromise. This means the response focuses on both:

- the department, government agency or private industry entity with the compromised cyber security
- any additional departments or agencies that have portfolio responsibilities impacted as a result of the compromise (e.g. interdependencies, such as any subsequent community or human based consequences).

FIGURE 5: An example of how entities may experience primary or secondary consequences as a result of another entity's cyber security compromise.


ENTITY EXPERIENCING A CONSEQUENCE
ENTITY WITH COMPROMISED CYBER SECURITY
ENTITY EXPERIENCING A CONSEQUENCE
ENTITY EXPERIENCING A CONSEQUENCE

7.14.2 Roles and responsibilities

7.14.2.1 Entity experiencing a consequence

- Manage consequences for areas of portfolio responsibility, as defined in the State Emergency Management Plan.
- Provide strategic and management advice about actual, emergent and cascading consequences on areas of portfolio responsibility to the Emergency Management Commissioner and Class 2 State Controller – Cyber Security and/or Deputy Class 2 State Controller – Cyber Security, via the State Consequence Coordinator. This may be completed direct, or as a part of the State Emergency Management Team.
- Engage business continuity arrangements as required.

7.14.2.2 Entity with compromised cyber security

- Log any risks not remediated during the emergency in an internal risk register and manage in accordance with the internal risk management framework.

7.14.2.3 Emergency Management Commissioner

- Coordinate before, during and after major emergencies, including the consequence management of consequences of an emergency as defined in the *Emergency Management Act 2013*.
- Identify and engage early with departments and government agencies with potential consequences in consultation with the Class 2 State Controller – Cyber Security. Where appropriate, this should include a State Emergency Management Team meeting, or a smaller group of impacted or potentially impacted departments and government agencies if greater sensitivity is required.
- Request departments or agencies report on the impact and consequences of the emergency on their area of responsibility, identifying any emerging issues and actions to resolve these. This may be completed direct, or as a part of the State Emergency Management Team.

This information forms the basis of intelligence that is used to brief the Minister for Emergency Services and the State Crisis and Resilience Council or any delegated committee (such as the State Crisis and Resilience Council's Major Emergency Inter-Departmental Committee).

Government departments and government agencies can also use this report to brief their departmental executives and respective minister/s.

During a large-scale emergency, the Premier and/or Cabinet may choose to utilise a Cabinet subcommittee to provide Whole of Victorian Government ministerial oversight.

7.14.2.4 Class 2 State Controller – Cyber Security

- Consider identified consequences, and the progress of their management, in decision-making.

7.14.2.5 State Emergency Management Team

- Develop a state strategic plan with high-level actions for agencies to manage consequences. This plan should identify the potential consequences of emergencies and develop mitigation and response strategies to reduce impacts on Victorians.
- The team includes:
  - Emergency Management Commissioner (Chair)
  - Emergency Management Commissioner Executive Officer
  - Class 2 State Controller – Cyber Security
  - State Consequence Coordinator
  - Senior Police Liaison Officer
  - a senior member of each impacted department or government agency
  - a senior member of each key support agency
  - others as determined by the Emergency Management Commissioner and Class 2 State Controller – Cyber Security, for example, relevant individual agencies or representatives of business, industry, or community groups.

7.14.2.6 National Office of Cyber Security – Cyber Security Response Coordination Unit

- Support the Victorian government to manage consequences that may impact other states and territories.

7.15 Relief

7.15.1 Summary

Relief is the provision of assistance to meet the essential needs of individuals, families and communities during and in the immediate aftermath of an emergency. Relief is informed and supported by consequence management, which supports strategic decision-making before, during and after a cyber security emergency.

In the context of a cyber security emergency, relief activities could include support to individuals to manage the impact of a data breach that involves the disclosure of personal information and identity documents.
Support could include:

- cancelling identity documents.
- replacement of identity documents.
- providing personal security to mitigate any threats to personal safety.
- counselling and other support services to help address trauma.
- providing support for household or personal needs in the event of reduced access to essential supplies/services.

7.15.2 Roles and responsibilities

7.15.2.1 Departments and government agencies

- Align cyber security relief arrangements with those outlined in the State Emergency Management Plan which are applicable to all emergency types. Specifically, these arrangements include Table 11: 'Specified relief activities and relief coordinating agency' and Table 12: 'Relief coordination' of the State Emergency Management Plan, which detail the range and types of assistance, and the providers of each, to support community relief during and immediately after emergencies.
- Coordinate relief activities in accordance with the appropriate relief tier as defined in the State Emergency Management Plan.

7.16 National cyber security incident

7.16.1 Summary

Victoria's categorisation of incidents relates to incidents that have consequences for Victorians. Separately, the Cyber Incident Management Arrangements for Australian Governments outlines the declaration of a national cyber security incident which activates the arrangements. These arrangements include coordinating action during a national cyber security incident and de-escalating a declared national cyber security incident.

The declaration of the national cyber security incident occurs alongside, and does not replace, Victoria's state-based classification and response to any incident. National cyber security incidents can:

- significantly impact, or have the potential to significantly impact, multiple Australian jurisdictions
- require a coordinated inter-jurisdictional response.

The Cyber Incident Management Arrangements for Australian Governments outlines roles and responsibilities for the following stakeholders in the event of a national cyber security incident:

- State and Territory Governments and their law enforcement (which for the Victorian Government is Victoria Police)
- the Commonwealth Government, including the:
  - Australian Cyber Security Centre and the Australian Signals Directorate State Office, Melbourne
  - Australian Department of Home Affairs
  - Department of Prime Minister and Cabinet
  - Australian Federal Police
  - National Cyber Security Coordinator, supported by the National Office of Cyber Security within the Australian Department of Home Affairs
  - National Emergency Management Agency.
- businesses and the community.

7.16.2 Roles and responsibilities

7.16.2.2 National Emergency Management Agency

- Convene the Australian Government Crisis and Recovery Committee to bring together Australian Government agencies.
- Convene the National Coordination Mechanism, as required.

7.16.2.3 Department of Government Services

- Lead agency for Victoria, for National Cyber Security Incidents.

8 Cyber security emergency recovery

8.1.1 Summary

In a cyber security context, recovery is the process of returning an affected system or service to its proper level of functioning. The recovery phase can occur concurrently with the response phase. Depending on the emergency, recovery activities may include the ongoing management of consequences.[23]

Specific roles and responsibilities for the transition to recovery, the delivery of recovery coordination and recovery activities are set out in the State Emergency Management Plan.

Where an emergency has had a broad impact across social, economic, built, natural and Aboriginal culture and healing environments, the relevant Recovery Lead Agency will lead recovery activities with assistance from Recovery Support Agencies.

Cyber security emergencies can have consequences across environments and result in new forms of emergency. This may include energy, critical infrastructure distribution, natural gas or reticulated water and wastewater emergencies. The recovery programs for these emergencies may be complex and are addressed under the respective emergency's arrangements.

8.1.2 Social recovery

Cyber security emergencies can have consequences that may have adverse health, wellbeing and community cohesion impacts on individuals and communities, such as:

- physical injuries, illness, permanent disability and death
- psychosocial impacts
- mental health impacts
- increased strain on the health system or a situation where the health system is overwhelmed
- community concern, especially when the cause and extent of the health emergency is unknown
- concerns about returning to 'normal' life following the emergency
- disruptions to cultural practices.

At a community cohesion level, consequences of a cyber security emergency may lead to:

- social division
- public protests and violence
- mistrust of government.

[23] Adapted from the State Emergency Management Plan.

8.1.3 Economic recovery

Businesses and local economies can suffer a range of setbacks after cyber security emergencies. These can include the loss of business and livelihoods as well as disruptions to supply chains and shifts in demand. Business owners may incur multiple hardships. These must all be considered as part of the recovery effort.

Activities in this line of recovery focus on how businesses and local economies can survive in the short-term and thrive in the long-term. It is critical to build on existing economic strengths and opportunities with a focus on tourism, primary producers, small businesses, medium and large business, industry and sectors.

8.1.4 Built recovery

Essential utilities, services and built infrastructure can all be impacted as a consequence of a cyber security emergency. This includes water and wastewater services, electricity, telecommunications, access to food and banking.

There are also significant state-owned assets, such as schools, health services, critical infrastructure and emergency management facilities that have cyber infrastructure that may require repair and restoration following a cyber security emergency.

Built environmental impacts can also lead to impacts for both the natural and Aboriginal cultural heritage and healing environments. Impacts to the natural environment will likely be managed through other State Emergency Management Plan sub-plans with relief and recovery responsibilities coordinated by relevant lead agencies.

8.1.5 Aboriginal culture and healing

Cyber security emergencies can have consequences on Victoria's First Peoples including:

- disruption of service provision through Aboriginal community-controlled organisations and Traditional Owner corporations
- data sovereignty
- theft of sensitive cultural heritage information and traditional knowledge
- delays in critical care
- impacts on land and resources management.

This can have adverse health impacts on Victoria's First Peoples as well as reveal sensitive information of culturally sensitive places.

Victoria's First Peoples may also be a target for disinformation, phishing attacks and harassment relating to communities, culture or land rights.

8.1.6 Roles and responsibilities

8.1.6.1 Emergency Recovery Victoria

- Coordinates state and regional recovery, as delegated by the Emergency Management Commissioner. Emergency Recovery Victoria partner with all levels of government, businesses and not-for-profit organisations to enable locally driven and locally delivered recovery.
- Establish recovery monitoring of natural and cultural heritage values, in consultation with all affected communities, including Victoria's First Peoples and Traditional Owner groups.

8.1.6.2 Impacted councils

- Councils are responsible for municipal recovery coordination, including coordination of local recovery activities and post-emergency needs assessment to determine long-term recovery needs.

8.1.6.3 Entity with compromised cyber security

- Implement disaster recovery arrangements to assist with returning impacted systems and services to normal operation as soon as possible following an incident.
- Liaise with the Victorian Management Insurance Authority or other cyber insurance provider to determine what support for recovery is available under a relevant insurance policy.
- Prepare a recovery plan (depending on the type and severity of incident, in conjunction with advisors in business continuity and IT services advisers) which details:
  - the approach to recovering IT networks, systems and applications once containment and eradication is complete
  - a plan to restore systems to normal operation
  - a process of continual monitoring to confirm that the affected systems are functioning normally
  - how to remediate vulnerabilities to prevent similar incidents (if applicable).

- The recovery plan may, in some circumstances, include the finalisation of a related criminal investigation (including forensic evidence collection), which needs to occur before recovery is possible.
- Confirm the threat has been eradicated and return affected systems/services to normal function, by testing systems/services to confirm expected functionality.
- Determine any stakeholder communication requirements.

8.2 Stand down

8.2.1 Summary

This section details the process for standing down the emergency.

8.2.2 Roles and responsibilities

8.2.2.1 State Recovery Coordinator or delegate

- Advise the Incident Management Team that it is acceptable to stand down, following the implementation and execution of an agreed recovery plan.

8.2.2.2 Entity Incident Manager

- Gather copies of all notes taken during the response to assist with a post-emergency review.

9 Lessons and evaluation

9.2.1 Summary

This step is one of the most important phases in the incident response process. Incident Management Teams use the evaluative process to continually improve.

9.2.2 Roles and responsibilities

9.2.2.1 Entity with compromised cyber security

- Conduct a review to document learnings and insights of the relevant mitigation, response and recovery activities, including root cause and vulnerability analysis (what worked well and any opportunities for improvement).
- Following the review:
  - share outcomes with a wide range of stakeholders, including the Cyber Incident Response Service
  - monitor implementation of relevant actions arising from the review
  - update the cyber security incident response plan to reflect better practice in cyber security incident response activities
  - develop an action plan with new or modified mitigation or preparedness activities to address identified areas for improvement.

9.2.2.2 Cyber Incident Response Service

- Undertake a review to document learnings and insights of the relevant mitigation, response and recovery activities, related to the Cyber Incident Response Service and wider emergency response (what worked well and any opportunities for improvement).
- Following the review:
  - analyse insights and identify lessons from assurance activities
  - provide opportunities for all relevant stakeholders to access and utilise identified lessons
  - assess identified lessons for change/improvement activities, including updating this Plan to reflect better practice in the response to cyber security emergencies.

9.2.2.3 Emergency Recovery Victoria

- Coordinate recovery as well as the monitoring and evaluation of the progress and success of recovery activities according to long-term outcomes.
- Use an outcomes-based approach to monitor and evaluate the impact of recovery programs aligned to the Inspector-General for Emergency Management's Assurance Framework for Emergency Management. Three key elements underpin this approach:
  - **Long term recovery outcomes:** making clear, unambiguous statements about what long-term recovery looks like for each recovery line with criteria for assessing the success of recovery programs against these outcomes.
  - **Evaluation:** collating data collected through ongoing monitoring processes, gathering additional data and information to draw insights and conclusions about the impact of the recovery programs.
  - **Monitoring:** undertaking the regular and ongoing assessment of efforts, such as the execution of key activities within time and budget and delivery of key outputs.

10 Appendices

10.1 Appendix A – Acronyms

This Plan uses full references instead of acronyms to support readability. However, in the event of a compromise of cyber security, acronyms are commonly used. Appendix A provides table of acronyms is prepared to support the reader's understanding in these contexts.

TABLE 6: List of acronyms

Acronym	Expanded acronym used within this Plan
ACSC	Australian Cyber Security Centre
AGCMF	Australian Government Crisis Management Framework
AGCRC	Australian Government Crisis and Recovery Committee
AIIMS	Australasian Inter-Service Incident Management System
BCP	Business Continuity Plans
BIL	Business Impact Level
C2SC – CS	Class 2 State Controller – Cyber Security
CA	Control Agency
CAOiC	Control Agency Officer in Charge
CCP	Chief Commissioner of Police
CDC	Cyber Defence Centre
CI	Critical Infrastructure
CIRS	Cyber Incident Response Service
CISC	Cyber and Infrastructure Security Centre
CIMA	Cyber Incident Management Arrangements for Australian Governments
CISO	Chief Information Security Officer
CIMP	Cyber Incident Management Plan
CSIRP	Cyber Security Incident Response Plans
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	Essential Eight
EMC	Emergency Management Commissioner
EM Act 2013	*Emergency Management Act 2013* (Vic)
EM Act 1986	*Emergency Management Act 1986* (Vic)
EMJPIC	Emergency Management Joint Public Information Committee
EMV	Emergency Management Victoria
ERV	Emergency Recovery Victoria
IAP	Incident Action Plan
IC	Incident Controller
ICT	Information Communications Technology

IMT	Incident Management Team
IR	Incident Response
IRAP	Information Security Registered Assessors Program
ISM	Australian Government Information Security Manual
MSPs	Managed Service Providers
NCM	National Coordination Mechanism
NCSC	National Cyber Security Committee
NEMA	National Emergency Management Agency
NIST	National Institute of Standards and Technology
NOSC	National Operations Sub-Committee
OVIC	Office of the Victorian Information Commissioner
PDP Act	*Privacy and Data Protection Act 2014*
PIO	Public Information Officer
PSPF	Protective Security Policy Framework
RC	Regional Controller
(C2) SCT – CS	(Class 2) State Control Team – Cyber Security
SC	See *C2SC – CS*
SCC	State Control Centre
SCRC	State Crisis and Resilience Council
SEMP	State Emergency Management Plan
SITREP	Situation Report
SOC	Security Operations Centre
SOCI Act	*Security of Critical Infrastructure Act 2018*
SPLO	Senior Police Liaison Officer
SRN	Sector Resilience Network
TLP	Traffic Light Protocol
VERA	Victorian Emergency Risk Assessment
VGRMF	Victorian Government Risk Management Framework
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

10.2 Appendix B – Common sources of cyber security compromise

TABLE 7: Summary of common sources of cyber security compromise

Type	Description	Suggested 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 virus, worm, trojan horse, or other code-based malicious entity that successfully infects a host.	Immediately remove the infected device/s from the network to limit the spread of malware. Capture all available logs relevant to the device. Isolate the devices while containment activities are confirmed, and eradication efforts are determined.
Denial of service (DoS) and distributed denial of service (DDoS) attacks	Overwhelming an ICT 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 and monitoring accounts for any unauthorised access.
Data breach	Unauthorised access to sensitive or personally identifiable information.	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 Office of the Victorian Information Commissioner's Managing the Privacy Impacts of a Data Breach

10.3 Appendix C– Sector Resilience Networks

> Sector Resilience Networks are a key interface between business and government. They link critical infrastructure sectors under Victoria's Critical Infrastructure Resilience Strategy.

10.3.1 Sector Resilience Networks

→ Sector Resilience Networks, or another key stakeholder group, may be convened by responsible government departments to provide a forum for business and government to discuss sector challenges, dependencies, opportunities and best practice.

10.3.2 Department of Government Services

→ Department of Government Services works with Sector Resilience Networks to provide critical infrastructure owners and operators with advice on cyber security emergency risks and mitigation strategies.

10.3.3 Emergency Management Victoria

→ The Critical Infrastructure Resilience Sectors Forum is chaired by Emergency Management Victoria and includes membership of the Chair of each Sector Resilience Network.

TABLE 8: Overview of Sector Resilience Networks

Sector Resilience Network		Responsible Portfolio Department
1	Water	Department of Energy, Environment and Climate Action
2	Transport	Department of Transport and Planning
3	Energy	Department of Energy, Environment and Climate Action
4	Food and grocery	Department of Jobs, Skills, Industry and Regions
5	Banking and finance	Department of Treasury and Finance
6	Government	Department of Premier and Cabinet
7	Telecommunications	Department of Government Services
8	Health	Department of Health

10.4 Appendix D – State Emergency Management Priorities

> The State Emergency Management Priorities are extracted from the State Emergency Management Plan.

TABLE 9: Summary of relevant State Emergency Management Priorities

State Emergency Management Priorities
Protection and preservation of life and relief of suffering is paramount. This includes: → Safety of emergency response personnel; and → Safety of community members including those most at risk in emergencies, residents, and visitors/tourists.
Issuing of community information and community warnings detailing incident information that is timely, relevant and tailored to assist community members make informed decisions about their safety.
Protection of critical infrastructure and community assets that support community resilience.
Protection of residential property as a place of primary residence.
Protection of assets supporting individual livelihoods and economic production that supports individual and community financial sustainability.
Protection of environmental and conservation assets that considers the cultural, biodiversity, and social values of the environment.

10.5 Appendix E – Summary of threat intelligence products

TABLE 10: Summary of threat intelligence products

Product	Summary	Audience
Alert	Tactical and technical intelligence that contains practical and actionable information which requires urgent action and attention. An alert is prepared in response to or forewarning of an issue, vulnerability or threat campaign.	IT practitioners
Advisory	Informs situational awareness, monitoring and consideration. Prepared in response or forewarning of an issue, vulnerability or threat campaign. Can contain practical and actionable information.	IT practitioners
Intelligence brief	Analysis of a cyber security trend, issue or problem with potential Whole of Victorian Government impacts.	IT practitioners
Intelligence summary	Intelligence and actions of an ongoing cyber security incident that is prepared when an issue becomes larger in scope (for example, has a multi-agency impact).	Cyber leads Executives Communications Management
Situational report	Regular updates on a specific cyber security risk, issue or incident, designed to inform a common understanding of a situation, including details of current priorities and future actions.	Cyber leads Executives Communications Management

10.6 Appendix F – Frameworks for cyber security maturity

10.6.1 Australian Cyber Security Centre's 'Essential Eight' Maturity Model

The Australian Cyber Security Centre has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents. These help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies is the 'Essential Eight'. The model outlines three levels of maturity for each of the 8 categories:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks.

No single mitigation strategy is guaranteed to prevent cyber security incidents. However, properly implementing the Essential Eight is so effective at mitigating targeted cyber intrusions that the Australian Cyber Security Centre considers this to be the new cyber security baseline for all organisations.

For organisations that use the Australian Government Information Security Manual, the Australian Cyber Security Centre provides mapping between the Essential Eight and the security controls contained in the Information Security Manual.

10.6.2 Cyber Security Framework, National Institute of Standards and Technology (NIST; USA)

The NIST Cyber Security Framework provides a comprehensive approach to improving cyber maturity, including alignment to the Essential Eight, while meeting obligations within the Victorian Protective Data Security Framework.

The NIST Cyber Security Framework is aligned to ISO27001 and integrates industry standards and best practices to help organisations manage their cyber security risks.

This framework provides a set of cyber security activities, desired outcomes and applicable references that are common across critical infrastructure sectors. It provides a common language to develop a shared understanding of sector-specific cyber security risks.

This framework can be used by organisations that already have extensive cyber security programs, as well as those just beginning to think about putting cyber security management programs in place.

This framework not only helps organisations understand their cyber security risks (threats, vulnerabilities and impacts), but also how to reduce these risks with customised measures.

This framework also helps organisations respond to and recover from cyber security incidents, prompting them to analyse root causes and consider how they can make improvements.

10.6.3 Protective Security Policy Framework

The Protective Security Policy Framework helps Australian Government entities to protect their people, information and assets, both at home and overseas.

It sets out the Australian Government's protective security policy and supports entities to effectively implement this policy across:

- security governance
- information security
- personnel security
- physical security.

10.6.4 Victorian Government Risk Management Framework

Victorian Government Risk Management Framework, published by the Department of Treasury and Finance, applies to departments and public bodies covered by the *Financial Management Act 1994*.

This framework describes the minimum risk management requirements agencies must meet to demonstrate that they are managing risk effectively, including shared and state significant risk.

10.6.5 Victorian Protective Data Security Framework and Standards

Published by the Office of the Victorian Information Commissioner, this is Victoria's overall scheme for managing protective data security risks in Victoria's public sector. It also consists of the:

- assurance model
- supplementary security guides and supporting resources.

10.6.6 Australian Energy Sector Cyber Security Framework

The Australian Energy Sector Cyber Security Framework has been developed through collaboration with industry and government stakeholders, including the Australian Energy Market Operator, Australian Cyber Security Centre, Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations.

This framework leverages recognised industry frameworks such as the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model and the National Institute of Standards and Technology Cyber Security Framework and references global best practice control standards (such as ISO/IEC 27001).

This framework also incorporates Australian-specific control references, such as the Australian Cyber Security Centre 'Essential Eight' Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles and the Notifiable Data Breaches scheme.

10.7 Appendix G – Useful steps in confirming the presence of a cyber security incident

TABLE 11: Summary of steps to confirm the presence of a cyber security incident

Action	Description
Update resources	Ensure you have access to the latest: → network diagrams → IP addressing schemas → port lists → system logs → documentation that may include system designs/architecture, security plans, GPO configuration, etc.
Review log entries and security alerts	Determine if there are any unusual entries or signs of suspicious behaviour on the network or applications.
Develop Standard Operating Procedures (SOPs) for different operating systems	For Microsoft Windows workstations, follow a SOP on what to look for or review (such as, specific event log sources, the types of events to search for, etc.). The same applies for Linux and Unix operating systems.
Consult with network and application experts	Determine if there is a legitimate explanation for the unusual or suspicious activity that has been observed.
Conduct research	Research and review any open-source materials (including via internet search engines) relating to the unusual or suspicious activity (for example, consider performing a search on any unusual filenames that are observed on the network).
Develop a watch list/monitor list	Develop a list where suspected accounts or IPs can be added to monitor their ongoing activity.
Conduct investigations securely through a third party	**IMPORTANT:** Do not 'ping' or try to communicate with a suspected IP address or URL from your own network, as you may tip off the attacker that you have detected their activity. This should be conducted by a third party that is able to conduct this activity securely and anonymously.

10.8 Appendix H – Contact details of key stakeholder agencies

TABLE 12: Contact details of key stakeholder agencies

Key Stakeholder	Phone	Emails (monitored during business hours)	Website
Australian Cyber Security Centre	**1300 CYBER1** (1300 292 371) Monitored 24/7	asd.assist@defence.gov.au	www.cyber.gov.au/report-and-recover/report
Cyber Incident Response Service	**1300 278 842** Monitored 24/7	cybersecurity@dpc.vic.gov.au	–
National Office of Cyber Security	–	General enquiries: cscsupport@homeaffairs.gov.au Consequence management enquiries: Cyber Security Response Coordination Unit, csrcu@homeaffairs.gov.au	https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/cyber-coordinator
Office of the Victorian Information Commissioner	**1300 00 OVIC** (1300 006 842) Monitored 9am-5pm, Monday to Friday	incidents@ovic.vic.gov.au	www.ovic.vic.gov.au/privacy/resources-for-organisations/information-security-and-privacy-incident-notification-form
Victorian Managed Insurance Authority	**03 9270 6900** Monitored 9am-5pm, Monday to Friday **1300 135 790** For after hours enquiries	claims@vmia.vic.gov.au	www.vmia.vic.gov.au
Victoria Police	If there is a threat to life or risk of harm, call **000**	–	www.police.vic.gov.au/report-cybercrime

10.9 Appendix I – Comparison of Whole of Victorian Government cyber security incident categories with Business Impact Levels

The Whole of Victorian Government cyber security incident categories are prepared as a comparable state-level equivalent to the Office of the Victorian Information Commissioner's entity-level Business Impact Levels.[24]

This means that the Whole of Victorian Government categories share similar terminology and characteristics to an internal department or government agency cyber security incident but at a state-scale.

Importantly, the two sets of categories are otherwise not directly related to each other. For example, a Business Impact Level 4 'serious' incident is considered serious for the department or government agency but does not automatically equate to a cyber security emergency at the state level).

TABLE 13: Comparison between incident categories and Business Impact Levels

For use at a Whole of Victorian Government scale		For use internally within a department or government agency[25]	
Severity level	**Whole of Victorian Government Category**	**Business impact**	**Business Impact Level**
1	Cyber security event	N/A	Business Impact Level 0
2	Minor cyber security incident	Minor	Business Impact Level 1
3	Limited cyber security threat or incident	Limited	Business Impact Level 2
4	Major cyber security threat or incident	Major	Business Impact Level 3
5	Critical cyber security incident		
6	Cyber security emergency	Serious	Business Impact Level 4
		Exceptional	Business Impact Level 5

[24] Victorian Protective Data Security Framework Business Impact Levels, Version 2.1, November 2019.

[25] While the requirements surrounding Business Impact Levels of the Victorian Protective Data Security Framework 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 Business Impact Levels in their own cyber security arrangements.

10.10 Appendix J – Summary of Australasian Inter-Service Incident Management System functions

In line with the State Emergency Management Plan, the Victorian Emergency Management Sector operates under the Australasian Inter-Service Incident Management System (AIIMS).

Smaller incidents may be manageable without formal activation of an Incident Management Team.

If the incident requires a team to manage the response effort, the Incident Controller, while remaining responsible for the overall response, will delegate functions to others.

At a minimum, the Incident Management Team will comprise of the Incident Controller, and they will be responsible for all the AIIMS functions.

The structure of the Incident Management Team required for each incident is tailored to the nature and severity of the incident.

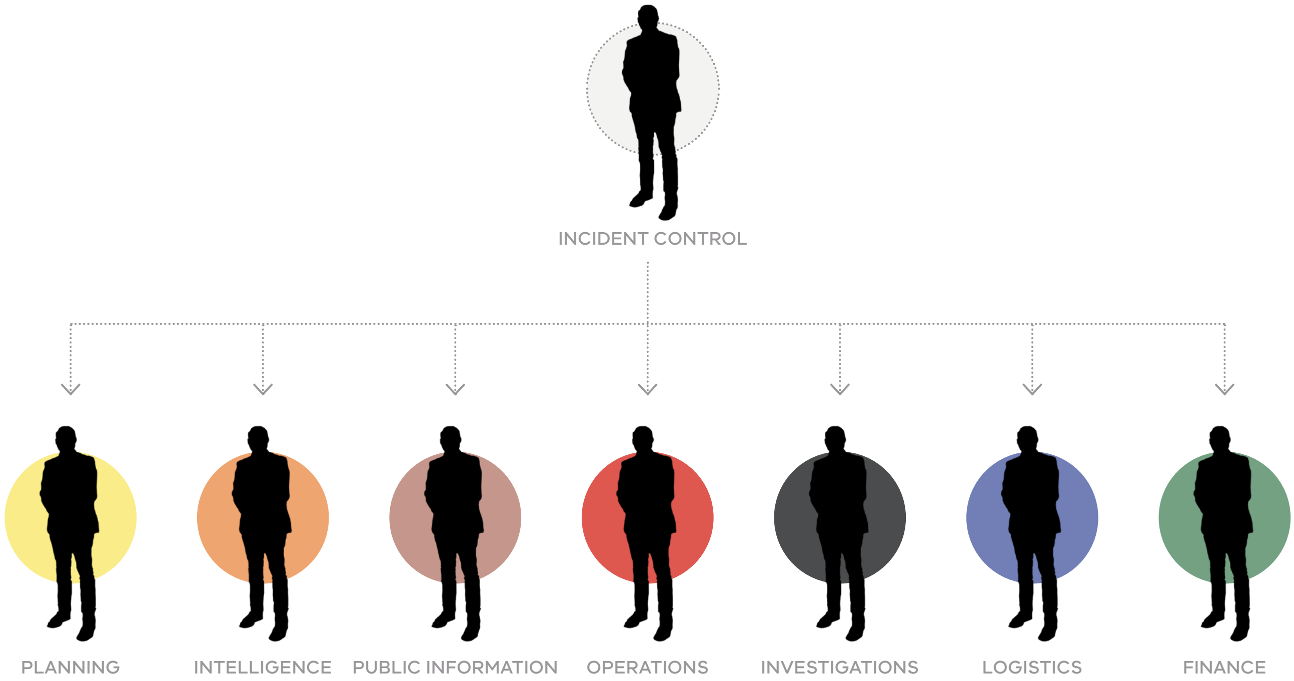


FIGURE 6: Australasian Inter-Service Incident Management System (AIIMS) functions

TABLE 14: Summary of Australasian Inter-Service Incident Management System functions

AIIMS Function	Description
Control	The management of all the activities necessary for the resolution of an incident.
Planning	The development of objectives, strategies and plans for the resolution of an incident based on the outcomes of collection and analysis of information.
Intelligence	The task of collecting and analysing information or data, to be recorded and disseminated as intelligence to support decision-making and planning.
Public Information	The provision of warnings, information and advice to the public and liaison with the media and affected communities.
Operations	The tasking and application of resources to achieve resolution of the incident.
Investigation	The task of conducting investigations to determine the cause of an incident and/or to determine factors that contributed to the impact of the incident or specific events.
Logistics	The acquisition and provision of human and physical resources, facilities, services and materials to support the achievement of incident objectives.
Finance	The task of managing: → accounts for purchases of supplies and hire of equipment → insurance and compensation for personnel, property and vehicles → the collection of cost data and provision of cost-effective analyses and providing cost estimates for the incident.
Lessons and evaluation[26]	The task of: → collecting and analysing observations → allocating improvement activities and monitoring progress of implementation.

[26] This is an additional function added in recognition of its importance in establishing a culture of continuous improvement in Victoria. It is not a recognised AIIMS function.

10.11 Appendix K – Demonstrating linkages with the Victorian Preparedness Framework

The Victorian Preparedness Framework, published by Emergency Management Victoria, sets out 21 core capabilities and their critical tasks as a foundation of how Victoria can mitigate, plan, prepare, respond to and recover from emergencies.

This section outlines the critical tasks relevant to cyber security emergencies and demonstrates how the critical tasks in this framework are addressed within this Plan. Certain critical tasks not relevant to cyber security emergencies have not been included in this list. For example, critical task 7.2 is 'Suppress, contain and extinguish major fires' and critical task 12.1 is to 'Conduct search operations to locate persons'.

TABLE 15: Summary of linkages with the Victorian Preparedness Framework

Victorian Preparedness Framework's critical task	Linkage with this Plan (heading or sub-heading)
1. Planning	
1.1 Share information with relevant stakeholders to assist effective emergency management planning	Threat intelligence Community and industry awareness and engagement
1.3 Identify, analyse and evaluate the likelihood and consequences of emergency events holistically, and document within relevant emergency risk assessments and relevant emergency management plans	Cyber security as a state significant risk
1.4 Community and agency stakeholders are engaged to explore, determine and implement mitigating actions to reduce or manage the likelihood and/or consequences of emergency events	Community and industry awareness and engagement
1.5 Communicate information to communities and agency stakeholders on the residual likelihood and consequences of an emergency after planning and mitigation is undertaken	Threat intelligence
1.6 Exercise, evaluate and review emergency management Plans regularly with agencies and community stakeholders using scenarios related to the relevant emergency risk profile.	Maintain and exercise plans and arrangements
2. Community information and warnings	
2.1 Provide information to people and communities on the risks, risk mitigation actions, and incident/events that may affect them	Community and industry awareness and engagement
2.3 Deliver timely, coordinated, accessible, tailored and relevant information and warnings to communities	Community and industry awareness and engagement

2.5 Plan for and deliver collaborative and proactive messaging to promote recovery in impacted communities	Community and industry awareness and engagement
3. Operational management	
3.1 Establish command and control to effectively deliver emergency management	Control
3.2 Activate established coordination networks to support operational response	Appendix C – Sector Resilience Networks
3.3 Identify and maintain facilities for emergency management activities	Control centre
4. Intelligence and information sharing	
4.5 Tailor and disseminate relevant intelligence to stakeholders	Threat intelligence
4.6 Provide relevant and actionable intelligence and predictive assessment	Threat intelligence
11. Impact assessment	
11.1 Gather information regarding extent of damage, immediate threats, loss of life and persons displaced	Analysis
17. Economic recovery	
17.2 Assist impacted businesses to access information and advice	Threat intelligence Community and industry awareness and engagement
18. Natural and cultural heritage rehabilitation	
18.6 Establish recovery monitoring of natural and cultural heritage values, in consultation with all affected communities, including Victoria's First Peoples and Traditional Owner groups	Recovery
19. Built recovery	
19.1 Undertake technical assessments for critical infrastructure	Analysis
21. Assurance and learning	
21.1 Undertake assurance activities before, during and after major emergency events	Lessons and evaluation
21.2 Analyse insights and identify lessons from assurance activities	Lessons and evaluation
21.3 Assess identified lessons for change / improvement activities	Lessons and evaluation
21.4 Monitor and measure improvement activities and outcomes	Lessons and evaluation
21.5 Provide opportunities for all personnel to access and utilise identified lessons	Lessons and evaluation

VICTORIA State Government

Government Services