EMV
EMERGENCY
MANAGEMENT
VICTORIA

VICTORIA
State
Government

Premier
and Cabinet

State Emergency Management Plan
Cyber Security Sub-Plan
Edition 2

Authorised and published by the Victorian Government Melbourne November 2020

This document is also available in Word and PDF format at www.emv.vic.gov.au

ISBN 978-1-925789-55-3 (pdf/online/MS word)

Acknowledgment of Country

The Department of Premier and Cabinet (DPC) acknowledges Aboriginal and Torres Strait Islander people as the Traditional Custodians of the land.

DPC 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.

Contents

1 Introduction

1.1 Purpose

This plan has been endorsed by the State Crisis and Resilience Council (SCRC) as a sub-plan to the State Emergency Management Plan (SEMP).

The plan outlines the arrangements for managing cyber security emergencies in Victoria.

The plan provides important information for government, business and the community about cyber security risks and emergency response mechanisms.

As the control agency for cyber security emergencies, the Department of Premier and Cabinet (DPC) has prepared and is responsible for the maintenance of this plan.

1.2 Objective

The plan outlines the arrangements for ensuring an integrated and coordinated approach to the State’s management of cyber security emergencies—spanning emergency mitigation, planning, preparedness, response and recovery activities.

By applying this plan and working together in an integrated and coordinated way, government, business and the community can reduce the risk of cyber security emergencies in Victoria.

1.3 Scope

The plan includes:

- description of the likelihood of cyber security emergencies and potential consequences to government, business and the community
- the policy and programs in place to mitigate these risks before, during and after an emergency
- the positions with accountability and the agencies responsible for managing specific strategies
- the multi-agency management arrangements at the national, state, regional and local levels
- links to sources of information where the reader can obtain further detail.

The plan provides strategic information about the Victorian arrangements for managing a cyber security emergency. It does not include detail about the operational activities of individual agencies.

1.4 Authorising environment

In 2019, the *Emergency Management Act 2013* (EM Act 2013) was amended to require the Emergency Management Commissioner to arrange for the preparation of a state emergency management plan, to provide for an integrated, coordinated and comprehensive approach to emergency management at the state level.

The EM Act 2013 requires the plan contain provisions providing for the mitigation of, response to and recovery from emergencies, and to specify the roles and responsibilities of agencies in relation to emergency management.

1.5 Activation of the plan

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

1.6 Audience

The SEMP recognises that emergency management—supporting communities to be safer and more resilient—is the shared responsibility of all Victorians, not just the emergency management sector.

The audience for this plan comprises government, business and the community of Victoria, and agencies within the emergency management sector.

This plan also provides information for Commonwealth Government organisations that may interact with Victoria's emergency management sector during a cyber security emergency.

1.7 Exercising and evaluation

This plan will be exercised within one year from the date of approval. The exercise will be evaluated, and where improvements to the emergency management arrangements in this plan are required, the plan will be updated and a revised version issued. Exercises will be conducted in accordance with the State Exercising Framework.

1.8 Review

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

This plan will be reviewed and updated every three years.

More frequent reviews may be undertaken if required, for example following the activation or exercising of the plan.

2 The emergency context

2.1 Cyber security risk environment

2.1.1 What is cyber security?

Society is increasingly drawing on digital and internet-enabled technologies to improve the functions of business and government, and to enrich our personal lives.

The prevalence of internet-enabled devices is rapidly expanding. Digital and social media are ubiquitous, and once labour-intensive processes are now handled seamlessly through advancements in automation, artificial intelligence and machine learning.

Although recent advancements in information communications technologies (ICT) have provided significant gains for modern society, they also give rise to various cyber security risks which have potential to harm the very people and institutions they were designed to benefit.

The Victorian Government defines cyber security as measures relating to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from external or internal threat.

It is commonly recognised that cyber security involves the protection of critical information and ICT infrastructure, including supervisory control and data acquisition (SCADA) systems and industrial control systems (ICS), through alignment of people, processes and tools with shared security goals.

2.1.2 Cyber security risks

The cyber security risks we face today are greater than ever before in our history.

Malicious attacks on computer systems are happening at an unprecedented rate. Australians report a new cyber security incident to the Australian Cyber Security Centre (ACSC) every 10 minutes. One in four of these incidents originates in Victoria.

Cyber security incidents involve cyber criminals, nation state actors, political ‘hacktivists’ and online vandals. They can significantly disrupt the delivery of critical infrastructure and essential services, as well as causing:

- damage to personal identity and reputation
- loss of economic, business or employment opportunities
- impact on emotional and psychological wellbeing.

The ripple effects from cyber security incidents can have significant and long-lasting consequences for government, industry and the community.

The Victorian Government treats cyber security as a state significant risk. We recognise the need for continued cooperation and collaboration across government, business and the community to support a cyber safe Victoria.

2.2 Cyber security emergencies

The Victorian Government defines a cyber security emergency as any cyber security incident that has the potential:

- to cause (or is causing) loss of life and extensive damage to property, infrastructure or the environment, and/or
- to have (or is having) significant adverse consequences for the Victorian community or a part of the Victorian community.

For the purpose of this plan, significant adverse community consequences arise when the organisation usually responsible for managing those consequences is unable to do so using normal business continuity arrangements; or adverse community consequences occur across multiple industries or locations and require management at the state level.

The arrangements for managing cyber security emergencies are detailed at section 3.

3 Managing cyber security emergencies

3.1 Emergency management priorities

The State Emergency Management Priorities underpin and guide all decisions at every phase of emergency management. These priorities apply to all aspects of the plan.

The priorities are:

- Protection and preservation of life and relief of suffering is paramount. This includes:
    - Safety of emergency response personnel and
    - Safety of community members including vulnerable community members 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.[1]
- 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.

3.2 Shared responsibilities

The SEMP recognises that emergency management is the shared responsibility of all Victorians, not just the emergency management sector. The 'shared responsibility' approach seeks to ensure:

- The interests, values and expectations of stakeholders in, or members of, communities are understood and considered.
- Ownership of the SEMP and responsibility for its implementation is broadly shared.

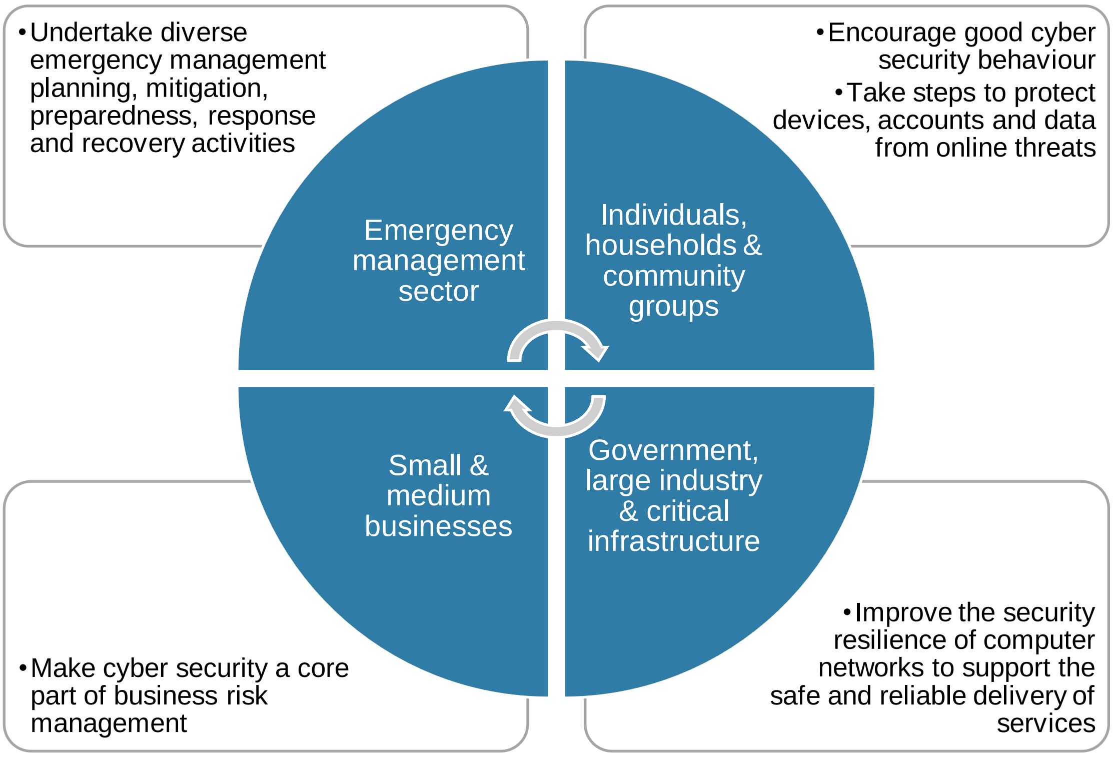
---

[1] This includes sharing accurate, relevant and timely cyber threat intelligence to support organisations in protecting their networks from potential harm.

Government, business and the community have a shared responsibility for minimising the risk of cyber security emergencies in Victoria, as reflected in Figure 1.

Although not legally binding, these principles should guide the actions of all Victorians to reduce the risk of cyber security emergencies.

Figure 1. Shared responsibilities for reducing cyber security risks to Victoria



Emergency management sector

- Undertake diverse emergency management planning, mitigation, preparedness, response and recovery activities

Individuals, households & community groups

- Encourage good cyber security behaviour
- Take steps to protect devices, accounts and data from online threats

Small & medium businesses

- Make cyber security a core part of business risk management

Government, large industry & critical infrastructure

- Improve the security resilience of computer networks to support the safe and reliable delivery of services

3.3 Mitigating cyber security risks

Every individual and organisation that uses digital systems or services can take meaningful steps to reduce their cyber security risk.

3.3.1 Advice for small to medium businesses, individuals, households and community groups

There are several steps that small to medium businesses, individuals, households and community groups can take to improve their cyber security.

The Victorian Government recommends the following steps as a minimum for improving cyber security:

- Regularly backup important files and data and keep a copy stored offline.
- Turn on automatic software updates; and apply software updates as soon as they are available.
- Use strong and unique passwords or passphrases to protect your accounts from unauthorised access.
- Enable multifactor authentication (sometimes called ‘two factor authentication’) on as many accounts as possible.
- Install and regularly update anti-virus software.
- Be careful when accessing links or opening attachments in emails from unknown senders.

Other useful information and tips about improving cyber security can be accessed via the following resources:

- https://www.cyber.gov.au/
- https://www.business.vic.gov.au/marketing-and-sales/eCommerce-and-digital-technology/cybersecurity

3.3.2 Mitigation strategies for government[2], large industry and critical infrastructure

Several resources are available to assist government, large industry and critical infrastructure organisations in mitigating cyber security risks. Two internationally recognised approaches are:

- The ‘Essential Eight’ Maturity Model provided by the ACSC.[3]
- The Cyber Security Framework provided by the National Institute of Standards and Technology (NIST), USA.[4]

Government, large industry and critical infrastructure owners and operators should adopt one or a combination of these approaches to reduce their cyber security risk.

If full alignment with these approaches is not possible, organisations should consider their cyber security risk profile (or an agreed industry standard) to determine the appropriate level of maturity to apply.

---

[2] For the purpose of this plan, ‘government’ includes local government authorities in Victoria.

[3] https://www.cyber.gov.au/publications/essential-eight-maturity-model

[4] https://www.nist.gov/cyberframework

Essential Eight Maturity Model

The Essential Eight Maturity Model is informed by the ACSC's experience in responding to cyber security incidents, performing vulnerability assessments and penetration testing Australian Government organisations.

Although no single mitigation strategy is guaranteed to prevent cyber security incidents, properly implementing the Essential Eight is so effective at mitigating targeted cyber intrusions that the ACSC considers this to be the new cyber security baseline for all organisations.

To assist organisations in determining the maturity of their implementation of the Essential Eight, three maturity levels have been defined for each mitigation strategy. The maturity levels are defined as:

- Maturity Level One: Partly aligned with the intent of the mitigation strategy.
- Maturity Level Two: Mostly aligned with the intent of the mitigation strategy.
- Maturity Level Three: Fully aligned with the intent of the mitigation strategy.

The ACSC recommends that organisations should aim to reach Maturity Level Three for each mitigation strategy.

Appendix 4.2 provides technical information about the Essential Eight mitigation strategies.

Note: For organisations that use the Australian Government Information Security Manual (ISM), the ACSC provides mapping between the Essential Eight and the security controls contained in the ISM - https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-ism-mapping

The NIST Cyber 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.

The 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 that allows staff at all levels within an organisation—and at all points in a supply chain—to develop a shared understanding of their cyber security risks.

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

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

The 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.

For organisations within the Victorian public sector, the NIST Cyber Security Framework provides a comprehensive approach to improving cyber maturity, including alignment to the Essential Eight, whilst meeting obligations within the Victorian Protective Data Security Framework.

3.4 Preparedness

3.4.1 Governance

Cyber security governance arrangements are continually maturing at all levels of government and private industry.

Commonwealth Government support

The Commonwealth Government sets Australia's national cyber security strategy and drives cyber security policy reform via the Department of Home Affairs.

Australia's *Cyber Security Strategy 2020* promotes the protection of Australians, businesses and critical infrastructure from the most sophisticated threats, alongside action from businesses to secure their products and services and protect their customers from known cyber vulnerabilities.[5] Protecting critical infrastructure and systems of national significance is a key priority for the Department of Home Affairs.

The Commonwealth Government, via the ACSC, provides DPC with threat intelligence and advice about cyber security risks and vulnerabilities which can assist with mitigating a cyber security emergency.

During a cyber security emergency, DPC may request the ACSC provide technical knowledge and/or expertise to assist with managing the emergency.

National arrangements

By nature, cyber security emergencies may cross jurisdictional boundaries. The Victorian Government actively contributes to a national, cooperative approach to cyber incident and emergency planning.

Arrangements for responding to nationally significant cyber incidents are described in the *Cyber Incident Management Arrangements* (CIMA) for Australian Governments. These arrangements are explained at Section 3.8.

When a cyber security emergency has national implications, DPC will coordinate the sharing of situational updates and threat intelligence across jurisdictions via the ACSC and the National Cyber Security Committee.

Private industry engagement

The ACSC operates Joint Cyber Security Centres (JCSC) in most Australian states and territories. The JCSCs unite government, business and the cyber security research community in an open and cooperative environment.

The JCSCs facilitate rapid information sharing between governments and business and enable organisations to develop joint solutions to complex and shared cyber security problems.

DPC uses the Melbourne JCSC as a place to engage with private industry to share threat intelligence, exchange expert advice, and discuss strategies for mitigating and responding to cyber security emergency risks.

Victorian arrangements

The Victorian arrangements for managing cyber security emergencies are detailed throughout this plan and the broader SEMP.

---

[5] https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

3.4.2 Planning for cyber security emergencies

All government, large industry and critical infrastructure organisations should plan and prepare their response to a cyber security emergency.

The Victorian Government recommends that all government, large industry and critical infrastructure organisations should have an agreed organisational cyber incident response plan in place, which is regularly validated and improved through cyber security exercises.

The Victorian Government provides access to free templates and guides to assist organisations in developing and practicing their incident response plan. These resources are available online at https://www.vic.gov.au/cyber.

Although small to medium business, individuals, households and community groups are less likely to be directly impacted by a cyber security emergency, it is still important to protect valuable computer systems and data from being damaged or lost.

The ACSC provides practical tips for protecting your systems and data from harm. This information can be accessed via https://www.cyber.gov.au/acsc/view-all-content/advice.

This includes tips for backing up and restoring critical data, using anti-virus software, and activating multifactor authentication.

3.4.3 Threat intelligence sharing

Threat intelligence provides insight into cyber security risks, trends and issues that require mitigation in order to reduce the likelihood and impact of harm.

DPC develops threat intelligence to provide insight into the likelihood and consequence of cyber security emergencies in Victoria.

This intelligence is based on advice obtained through other government and private industry sources, including the ACSC, and through analysis of cyber incidents, risks and issues observed by DPC.

In anticipation of, or during a cyber security emergency, the Victorian Government will publish and distribute threat intelligence to assist government, industry and the community with mitigating cyber security risks.

This includes engaging Victoria’s critical infrastructure Sector Resilience Networks to share threat intelligence with Victoria’s critical infrastructure owners and operators, including vital critical infrastructure operators.

3.4.4 Sector Resilience Networks

A key interface between business and government is through the Sector Resilience Networks for each of Victoria’s critical infrastructure sectors.

Sector Resilience Networks are convened by government departments and provide forums for business and government to discuss sector challenges, dependencies, opportunities and best practice.

These sectors and their responsible portfolio departments are:

- Water – Department of Environment, Land, Water and Planning
- Transport – Department of Transport
- Energy – Department of Environment, Land, Water and Planning
- Food and grocery supply – Department of Jobs, Precincts and Regions
- Banking and finance – Department of Treasury and Finance
- Government – Department of Premier and Cabinet
- Communications – Department of Jobs, Precincts and Regions
- Health – Department of Health and Human Services.

DPC works with the Sector Resilience Networks to provide critical infrastructure owners and operators with advice on cyber security emergency risks and mitigation strategies.

3.4.5 Cyber security exercises

All government and business organisations, particularly critical infrastructure owners and operators, should regularly exercise their response to a cyber security emergency. Exercising provides a valuable opportunity to improve emergency management plans, policies and procedures.

DPC works with the critical infrastructure Sector Resilience Networks, the ACSC and various industry bodies to unite operational, technology, communications and policy experts from across government and industry to practise cyber security incident and emergency management arrangements.

The arrangements contained in this plan will be exercised across government and business organisations, at both the state and federal level.

3.5 Response

3.5.1 Control agency arrangements

DPC is the control agency for cyber security emergencies in Victoria. A cyber security emergency is a Class 2 Emergency under the *Emergency Management Act 2013* (Vic).

As a control agency DPC is responsible for:

- Providing Victoria's critical infrastructure owners and operators with advice about cyber security risks and mitigation strategies, and education on the state's cyber security emergency management arrangements.
- Advising the Emergency Management Commissioner on the existence of, or potential for, a cyber security emergency in Victoria (in line with the incident categories provided at Table 1).
- Working with organisations at the source of a cyber security emergency to develop and oversee the implementation of effective incident response plans, including strategies to contain and eradicate active cyber threats.
- Working with support agencies, including the ACSC, Victoria Police, other government departments and private business to control operational response activities.
- Supporting the Emergency Management Commissioner through provision of regular situation updates and expert cyber security advice.

DPC will also provide information and strategic advice to the Premier and Cabinet (including any Cabinet subcommittees), and SCRC on whole-of-government response activities for cyber security emergencies.

3.5.2 Escalation and notification

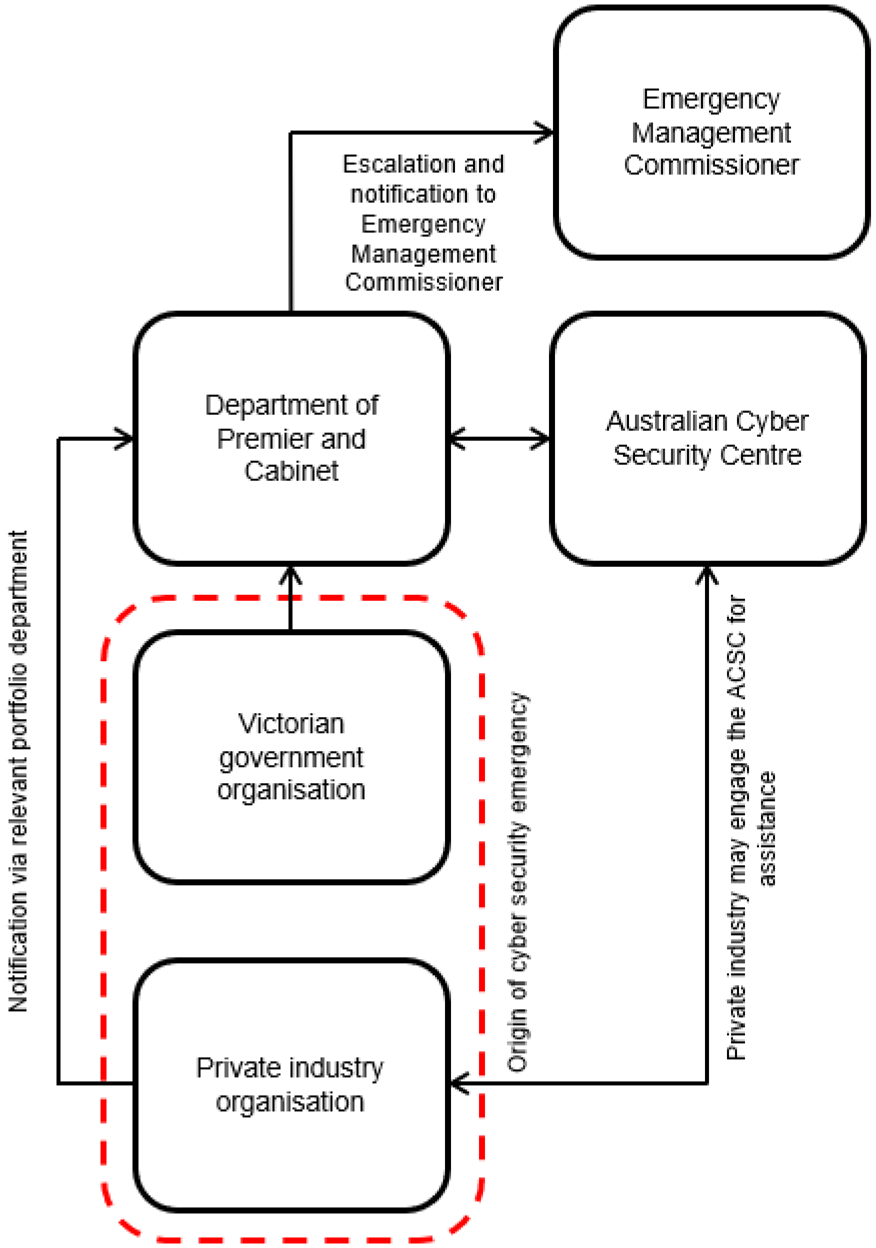
Private business organisations should report all cyber security incidents and emergencies to the ACSC on **1300 CYBER1 (1300 292 371) (24/7)**. Notifications should also be made to the relevant portfolio Victorian Government department (where applicable).

Victorian Government organisations should report all cyber security incidents to the Victorian Government Cyber Incident Response Service (CIRS) on **1300 CSU VIC (1300 278 842) (24/7)**, as well as notifying their relevant portfolio department.

More information about incident notification arrangements for Victorian Government organisations is contained in the Victorian Government Cyber Incident Management Plan - https://www.vic.gov.au/cyber-incident-management-plan

Figure 2 illustrates the escalation pathways for cyber security emergency notifications

Figure 2. Escalation pathways for cyber security emergency notifications


Emergency Management Commissioner
Escalation and notification to Emergency Management Commissioner
Department of Premier and Cabinet
Australian Cyber Security Centre
Notification via relevant portfolio department
Victorian government organisation
Private industry organisation
Origin of cyber security emergency
Private industry may engage the ACSC for assistance

3.5.3 Categories of cyber incidents

The Victorian Government uses a four-tier model to categorise cyber security incidents. The model reflects similar approaches taken by other Australian state and territory governments and can be overlayed with the categorisation model used by the ACSC.

Cyber security incidents are assessed according to the scale and severity of impacts they generate, and the extent to which they occur.

The four categories are:

- Cyber security event
- Cyber security incident
- Significant cyber security incident
- Cyber security emergency.

These categories are further explained in Table 1.

3.5.4 Cyber security emergency identification and assessment

Cyber security emergencies are most likely to originate in government or business settings, 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.

The occurrence of a cyber security emergency is determined by the Class 2 State Controller Cyber Security in consultation with the Emergency Management Commissioner, acting on advice from affected organisations and relevant portfolio government departments regarding:

- The potential for the situation to cause loss of life and extensive damage to property, infrastructure or the environment.
- The potential for the situation to have significant adverse consequences for the Victorian community or a part of the Victorian community.
- The capability and capacity of the affected organisation(s) to manage the cyber security issue.

Cyber security emergencies are unlikely to originate with small/medium businesses or households; although these groups may experience the adverse impacts and consequences of a cyber security emergency.

Table 1. Categories of cyber security incidents

CATEGORY	DESCRIPTION	TRIGGERS FOR ESCALATION
Cyber Security Event	A suspected (or unconfirmed) cyber incident with no impact to systems or services.	Substantial increase in cyber security alerts; or continued cyber security alerts with potential to breach security controls
Cyber Security Incident	Successful compromise of security controls. Minor impact to services, information, assets, reputation or relationships	Actual or high likelihood: • for limited or major impact to services; or • to affect multiple organisations; or • data breach.
Significant Cyber Security Incident	Successful compromise of security controls. Limited or major impact to services, information, assets, government reputation, relationships and/or the community (but not an emergency). Also any cyber incident that involves: • critical infrastructure or essential services; or • more than one organisation; or • a data breach.	A situation that: • has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment, or • has the potential to have or is having significant adverse consequences for the Victorian community or a part of the Victorian community.
Cyber Security Emergency	Serious or exceptional compromise of security controls that: • has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment; or • has the potential to have or is having significant adverse consequences for the Victorian community or a part of the Victorian community.	**When a cyber security emergency occurs, or is likely to occur, DPC will activate its control agency arrangements to provide the resources and capabilities necessary to respond effectively to the emergency.**

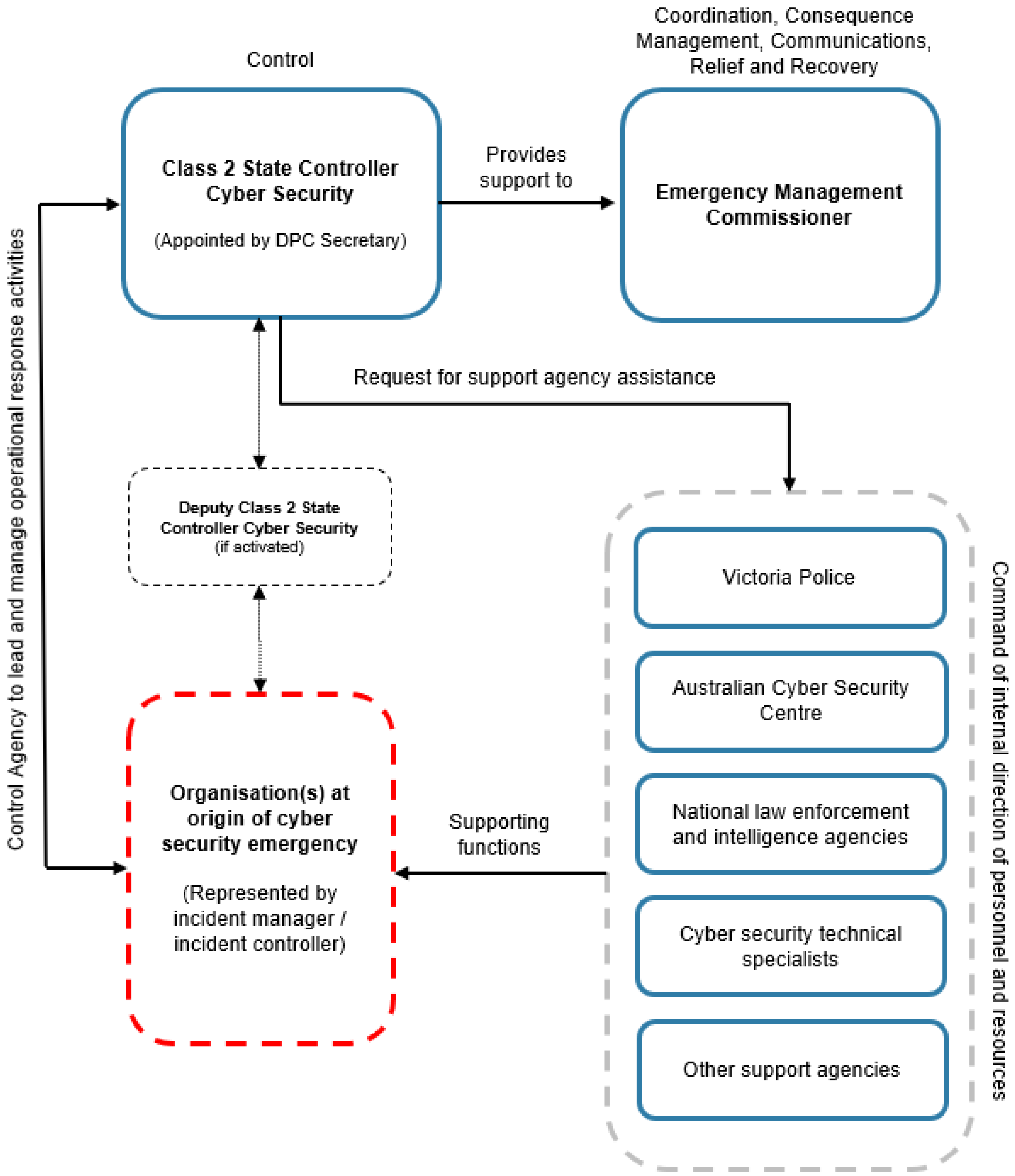
3.6 Coordination and control

Figure 3 illustrates the coordination and control arrangements for cyber security emergencies in Victoria.

Control of the emergency is provided by the Class 2 State Controller Cyber Security, with the Emergency Management Commissioner responsible for coordination, consequence management, communications, relief and recovery functions.

The DPC Secretary (as the control agency officer in charge) maintains a list of persons authorised to perform the role of Class 2 State Controller Cyber Security.

Figure 3. Control and coordination structure for cyber security emergencies


Control
Coordination, Consequence Management, Communications, Relief and Recovery
Class 2 State Controller Cyber Security
(Appointed by DPC Secretary)
Provides support to
Emergency Management Commissioner
Request for support agency assistance
Deputy Class 2 State Controller Cyber Security
(if activated)
Organisation(s) at origin of cyber security emergency
(Represented by incident manager / incident controller)
Supporting functions
Victoria Police
Australian Cyber Security Centre
National law enforcement and intelligence agencies
Cyber security technical specialists
Other support agencies
Control Agency to lead and manage operational response activities
Command of internal direction of personnel and resources

3.6.1 Control agency arrangements

DPC is the control agency for cyber security emergencies in Victoria. A cyber security emergency is a Class 2 Emergency under the *Emergency Management Act 2013* (Vic).

When a cyber security emergency occurs (or is anticipated), DPC will activate its cyber security emergency management arrangements (including this plan) to provide the resources and capabilities necessary to respond effectively to the emergency.

As a control agency DPC is responsible for:

- Advising the Emergency Management Commissioner on the existence of, or potential for, a cyber security emergency in Victoria (in line with the incident categories provided at Table 1).
- Working with organisations at the source of a cyber security emergency to develop and oversee the implementation of effective operational response plans, including strategies to contain and eradicate active cyber threats.
- Working with support agencies, including the ACSC, Victoria Police, other government departments and private business to control response activities.
- Supporting the Emergency Management Commissioner through provision of regular situation updates and expert cyber security advice.

DPC will also provide information and strategic advice to the Premier and Cabinet (including any Cabinet subcommittees), and SCRC on whole-of-government response activities for cyber security emergencies.

3.6.2 Emergency Management Commissioner

Under the *Emergency Management Act 2013* (Vic), the Emergency Management Commissioner has legislated management responsibilities across major emergencies. These include response coordination, ensuring effective control arrangements are established, consequence management and relief and recovery coordination.

The Emergency Management Commissioner coordinates the State's response to major emergencies through the following five key teams:

- State Coordination Team
- State Control Team
- State Emergency Management Team
- State Relief and Recovery Team
- Emergency Management Joint Public Information Committee.

Agency reporting to the Emergency Management Commissioner

During a cyber security emergency, the Emergency Management Commissioner may request agencies report on the impact and consequences of the event on their area of responsibility, identifying any emerging issues and actions to resolve these.

This information forms the basis of intelligence that is used by the Emergency Management Commissioner to brief the Minister for Police and Emergency Services and the SCRC.

Government departments and 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-government ministerial oversight.

3.6.3 Scaled response model

Cyber security emergencies can vary greatly in their scale and complexity.

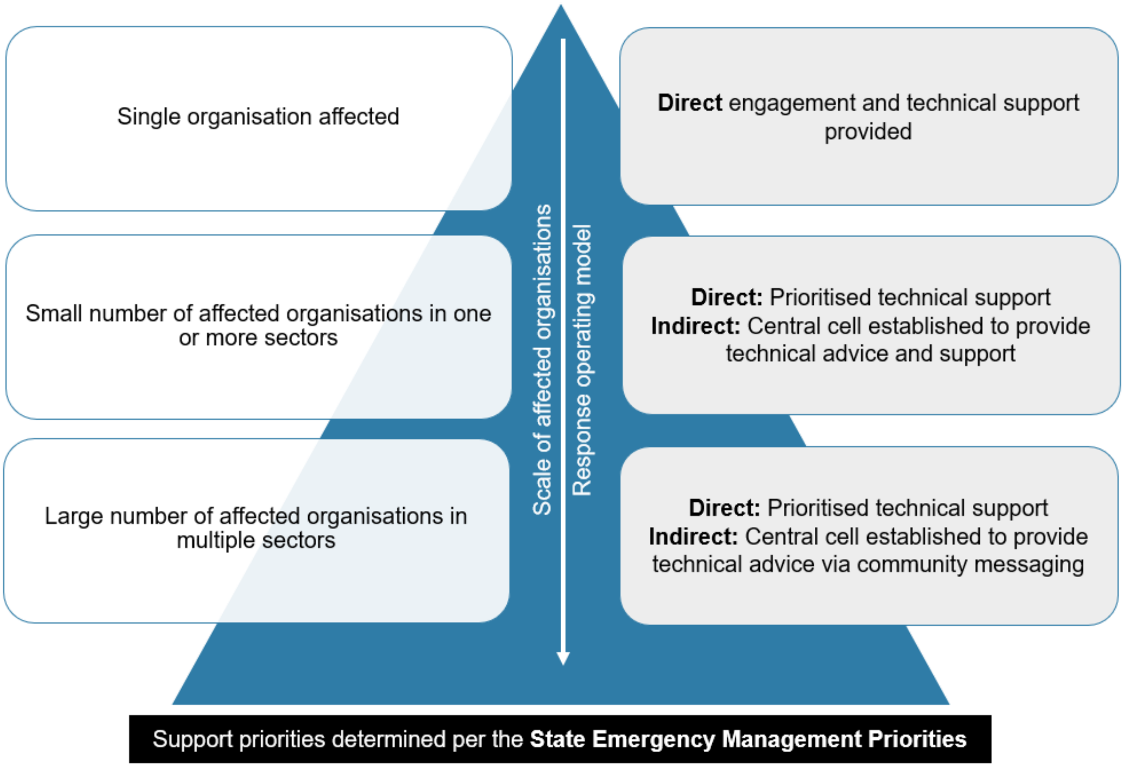
A cyber security emergency may affect the computer network of a single organisation, with the disruption of critical systems and services leading to adverse community consequences. Alternatively, a cyber security emergency may affect computer networks across multiple organisations and sectors at the state, national and international level.

In responding to a cyber security emergency, DPC will apply a scaled operating model that reflects the size and complexity of the situation. The intention of the model is to ensure that support is available to all organisations affected by a cyber security emergency, with response prioritisation decisions made in line with the State Emergency Management Priorities. This model is shown at Figure 4.

It is important to acknowledge that although DPC is the control agency for cyber security emergencies in Victoria, when dealing with private industry organisations it has no legal authority to give directions or compel organisations to act in preparation for, or response to, cyber security emergencies.

DPC will offer expert advice to support private industry organisations manage cyber security emergency risks, working in partnership with relevant portfolio government departments.

Figure 4. Scaled response model for cyber security emergencies


Single organisation affected
Small number of affected organisations in one or more sectors
Large number of affected organisations in multiple sectors
Scale of affected organisations
Response operating model
Direct engagement and technical support provided
Direct: Prioritised technical support
Indirect: Central cell established to provide technical advice and support
Direct: Prioritised technical support
Indirect: Central cell established to provide technical advice via community messaging
Support priorities determined per the **State Emergency Management Priorities**

3.6.4 Support agency arrangements

The Class 2 State Controller Cyber Security may request the assistance of support agencies, including the ACSC, to assist with managing cyber security emergencies.

Support requests may include, but are not limited to, providing expert technical advice and forensic services—which is common when responding to issues involving complex computer networks.

Although the composition of support agencies will vary depending on the circumstances of a cyber security emergency, it is broadly acknowledged that assistance will be required from:

- private industry cyber security experts
- Victorian Government Departments and Agencies
- ACSC
- Victoria Police
- Australian Federal Police.

3.6.5 Managing concurrent emergencies

It is highly likely that cyber security emergencies will occur in parallel with other major emergencies.

For example, a cyber security emergency involving power, water or communications infrastructure could disrupt the operations of multiple industries and sectors resulting in significant adverse community consequences.

When this occurs, the Emergency Management Commissioner will work with relevant agencies to prioritise response roles according to the SEMP and agreed priorities.

Factors such as the immediate threat or priority risk, the protection and preservation of life and the capabilities of agencies involved must be considered when determining control arrangements, particularly where several agencies may have defined responsibilities.

3.6.6 Transfer of control

Control agency responsibility may be transferred between agencies during an emergency, taking into consideration the above factors. Transfer of control occurs by arrangement between relevant controllers, as outlined in the SEMP. Where DPC transfers control to another agency, it will assume the role of a support agency, if required.

3.6.7 Criminal acts and Class 3 emergencies

DPC will refer any cyber security emergency which is a suspected criminal act to Victoria Police. Victoria Police is the lead agency for responding to criminal acts in Victoria. Subject to the circumstances of a cyber security emergency, Victoria Police may assume control agency responsibilities.

Where a Class 3 emergency occurs simultaneously with a Class 1 or Class 2 emergency, Victoria Police will maintain control of the Class 3 emergency, independently of the control arrangements of other the emergency.

If a cyber security emergency develops into a Class 3 emergency, then Victoria Police will assume control and lead the response.

3.7 Consequence management

Cyber security emergencies may generate significant adverse consequences for the Victorian community or a part of the Victorian community. In extreme circumstances, these consequences may result in the loss of life and extensive damage to property, infrastructure and/or the environment.

During a cyber security emergency, the Emergency Management Commissioner will appoint a State Consequence Manager. This role is responsible for providing advice about actual, emergent and cascading consequences before, during and after a major emergency. It works with the various emergency management teams to ensure a whole-of-government approach to the management of consequences.

3.8 National cyber security incidents and emergencies

The interconnected nature of modern computer networks increases the likelihood that any major cyber security incident will have impacts across multiple jurisdictions.

When a cyber security emergency occurs and has national implications, DPC and the Victorian Government will remain responsible for operational management of the response within Victoria.

Several arrangements exist to support DPC and the Victorian Government in coordinating response activity with other jurisdictions.

3.8.1 The National Cyber Incident Management Arrangements (CIMA)

The CIMA provides Australian governments with guidance on how they will collaborate in response to, and reduce the harm associated with, national cyber security incidents.[6]

If a cyber security incident or emergency impacts, or has the potential to significantly impact, multiple Australian jurisdictions, and/or requires a coordinated inter-jurisdictional response, the ACSC may declare a national cyber incident in consultation with cyber security leads from affected Australian governments.

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

3.8.2 Integrating with sector or industry coordination arrangements

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

3.8.3 National Cyber Security Committee

The National Cyber Security Committee is the peak cyber security coordination body for Australian governments. The National Cyber Security Committee provides strategic oversight and coordination of governments’ cyber security policies and operational capabilities nationally.

The National Cyber Security Committee’s role in responding to a national cyber security incident includes:

---

[6] The CIMA is available online at https://www.cyber.gov.au/acsc/view-all-content/news/expanded-agreement-incident-management-arrangements.

- 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.

The Victorian Government Chief Information Security Officer is Victoria's representative at the National Cyber Security Committee.

3.8.4 National emergencies

The Commonwealth Government coordinates management of crises at a national level through the Crisis Coordination Centre (CCC). The CCC provides whole-of-government situational awareness, planning and response options, and coordinated public messaging to decision makers during times of crisis, whether it is a natural disaster or a security incident.

Where a cyber security emergency has national connections, or impacts multiple states/territories simultaneously, DPC will work closely with the Commonwealth Government, the ACSC, 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.

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

3.9 Relief

The Emergency Management Commissioner is responsible for ensuring the provision of essential and urgent assistance to individuals, families and communities in and during the immediate aftermath of a cyber security emergency.

The Class 2 State Controller Cyber Security will support the Emergency Management Commissioner by advising on any relief requirements identified as a result of hazard response functions.

3.10 Recovery

The Emergency Management Commissioner is responsible for coordinating recovery activities via the State Recovery Coordinator and State Relief and Recovery Team.

Recovery means the assisting of persons and communities affected by emergencies to achieve a proper and effective level of functioning.

The Victorian Government's recovery outcomes, which guide recovery planning, programs and continued improvements to the recovery system, are:

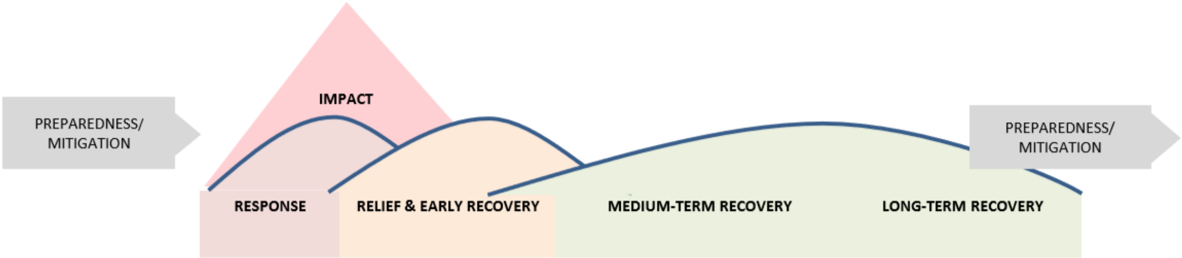
- Victorians are safe, resilient and healthy
- Victorians are connected to people, places and culture
- government responses and services are people-centred, adaptable and sustainable
- Victoria has thriving regions and a healthy environment.

In relation to a cyber security emergency, recovery activities will consider the built and natural environments, social and economic impacts and resulting community needs. This includes, but is not limited to:

- restoring essential services, infrastructure and lifelines that communities need to function
- enabling communities to adapt to the interruption
- providing tailored services that adapt when communities need them most
- bringing together people, resources, skills and capability

Figure 5 illustrates the phases of relief and recovery activities over time.

Figure 5. Emergency relief and recovery activities over time



3.11 Communications

The Emergency Management Commissioner is responsible for coordinating public, stakeholder and government communications, including all warnings and public information relating to cyber security emergencies. This role is supported by the Emergency Management Joint Public Information Committee (EMJPIC).

The nominated spokesperson for communications during a cyber security emergency will vary depending on the circumstances of the emergency, its consequences and existing media comment or other concurrent emergencies. Potential spokespersons include, but are not limited to:

- Victorian Premier or relevant Minister
- Emergency Management Commissioner
- Victorian Government Chief Information Security Officer
- Class 2 State Controller Cyber Security
- Senior Executive from Victorian Government portfolio departments or agencies affected by the consequences of a cyber security emergency.

The Class 2 State Controller Cyber Security, in conjunction with DPC Senior Executive, must authorise all public communications regarding cyber security emergencies.[7]

During cyber security emergencies with national implications—for example a cyber security emergency affecting multiple states and territories simultaneously—DPC and the Emergency Management Commissioner will coordinate public communications activities with the Commonwealth Government, including via the Department of Home Affairs.

---

[7] If there is an imminent threat to life and property and warnings must be issued urgently, regional controllers (if activated) can issue warnings to a community under threat, but they must notify the Class 2 State Controller Cyber Security as soon as possible after doing so

4 Appendices

4.1 Related plans, documents and services

DOCUMENT	LINK
Australian Government Information Security Manual	https://www.asd.gov.au
Critical infrastructure All Sectors Resilience Report	https://www.emv.vic.gov.au/
Critical Infrastructure Resilience Strategy	https://files-em.em.vic.gov.au/public/EMV-web/Critical-Infrastructure_Resilience_Strategy_Sept-2016.pdf.
Essential Eight Maturity Model	https://www.cyber.gov.au/publications/essential-eight-maturity-model
NIST Cyber Security Framework	https://www.nist.gov/cyberframework
State Emergency Management Plan	https://www.emv.vic.gov.au/responsibilities/semp
Strategies to Mitigate Cyber Security Incidents	https://www.asd.gov.au
Victorian Government Cyber Incident Management Plan	https://www.vic.gov.au/cyber-incident-management-plan
Victorian Government Cyber Security Strategy	https://www.vic.gov.au/victorian-government-cyber-security-strategy

4.2 Essential Eight overview

CONTROL	MITIGATION STRATEGY OVERVIEW[8]
Application control	Application control can prevent the execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
Patch applications	Security vulnerabilities in applications can be used to execute malicious code on systems. Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers to reduce risk of software exploit. Patch/mitigate computers with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest version of applications.
Configure Microsoft Office macro settings	Microsoft Office macros can be used to deliver and execute malicious code on systems. Configure Microsoft Office macro settings to block macros from the internet, and only allow vetted macros either in ‘trusted locations’ with limited write access or digitally signed with a trusted certificate.
User application hardening	Flash, ads and Java are popular ways to deliver and execute malicious code on systems. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
Restrict administrative privileges	Admin accounts are the ‘keys to the kingdom’. Adversaries use these accounts to gain full access to information and systems. Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Do not use privileged accounts for reading email and web browsing.
Patch operating systems	Security vulnerabilities in operating systems can be used to further the compromise of systems. Patch/mitigate computers (including network devices) with ‘extreme risk’ vulnerabilities within 48 hours. Use the latest operating system version. Do not use unsupported versions.
Multi-factor authentication	Stronger user authentication makes it harder for adversaries to access sensitive information and systems. Use multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.
Daily backups	Daily backups of important new/changed data, software and configuration settings, stored disconnected, should be retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

---

[8] Refer to https://www.cyber.gov.au/publications/essential-eight-maturity-model for full technical detail about each control and the desired maturity levels.

4.3 Glossary

Refer to the SEMP for a detailed list of emergency management terms and definitions used in Victoria - https://www.emv.vic.gov.au/responsibilities/semp.

TERM	DEFINITION
ACSC	Australian Cyber Security Centre.
CISO	For the purpose of this plan, this refers to the Victorian Government Chief Information Security Officer. The is the government executive responsible for promoting enhanced cyber security resilience across the Victorian Government.
Class 1 Emergency	A major fire or any other emergency for which the Metropolitan Fire and Emergency Services Board, the Country Fire Authority or the Victoria State Emergency Services Authority is the control agency under the State Emergency Response Plan.
Class 2 Emergency	A major emergency which is not – a) A Class 1 emergency b) A warlike act or act of terrorism, whether directed at Victoria or a part of Victoria or at any other State or Territory of the Commonwealth; or c) A hi-jack, siege or riot. (*Emergency Management Act 2013* section 3).
Class 2 State Controller Cyber Security	A person appointed as a Class 2 Controller for Cyber Security emergencies at the state tier under the *Emergency Management Act 2013* section 39.
Class 3 Emergency	A class 3 emergency means a warlike act or act or terrorism, whether directed at Victoria or part of Victoria or at any other State or Territory of the Commonwealth, or a hi-jack, siege or riot. Class 3 emergencies may also be referred to as security emergencies.
Consequence Management	The EM Act 2013 defines consequence management as the coordination of agencies that are responsible for managing or regulating services or infrastructure which are or may be affected by a major emergency. This includes agencies who engage the skills and services of non-government organisations
Control Agency	The agency: • primarily responsible for managing the response to the emergency • responsible for establishing the management arrangements for an integrated response to the emergency

Coordination	Coordination is the bringing together of people, resources, governance, systems and processes, to ensure effective response to and relief and recovery from an emergency.
Cyber security	The Victorian Government defines cyber security as measures relating to the confidentiality, availability and integrity of information and data that is processed, stored and communicated by electronic or similar means, protecting it and associated systems from external or internal threat.
Cyber security incident	A cyber security incident occurs when there is a breach of explicit or implied security policy that requires corrective action.
Cyber security emergency	A cyber security incident which causes major disruption to the services and operations of government, business and the community, and presents genuine risks to critical infrastructure and the safety of individuals and businesses.
Department	For the purpose of the SEMP, departments are Victorian Government departments, including those with portfolio responsibility for agencies with a role in emergency response.
Emergency	The actual or imminent occurrence of an event which in any way endangers or threatens to endanger the safety or health of any person in Victoria or which destroys or damages, or threatens to destroy or damage, any property in Victoria or endangers or threatens to endanger the environment or an element of the environment in Victoria including, without limiting the generality of the foregoing— a) an earthquake, flood, windstorm or other natural event; and b) a fire; and c) an explosion; and d) a road accident or any other accident; and e) a plague or an epidemic or contamination; and f) a warlike act or act of terrorism, whether directed at Victoria or a part of Victoria or at any other State or Territory of the Commonwealth; and g) a hi-jack, siege or riot; and h) a disruption to an essential service. (*Emergency Management Act* 2013 Part 1 section 3).
Emergency Management Sector	The sector comprising all agencies, bodies, departments and other persons who have a responsibility, function or other role in emergency management. (*Emergency Management Act* 2013 section 3).
Major Emergency	A major emergency is: a) A large or complex emergency (however caused) which – i. has the potential to cause or is causing loss of life and extensive damage to property, infrastructure or the environment

	ii. has the potential to have or is having significant adverse consequences for the Victorian community or a part of the Victorian community iii. requires the involvement of two or more agencies to response to the emergency. b) A Class 1 emergency c) A Class 2 emergency (*Emergency Management Act* 2013 section 3).
Recovery	Recovery means the assisting of persons and communities affected by emergencies to achieve a proper and effective level of functioning.
Relief	The provision of essential and urgent assistance to individuals, families and communities in and during the immediate aftermath of an emergency.
Resources	The people, equipment or services an agency requires to perform its emergency response role and responsibilities.
Response	Response is the action taken immediately before, during and in the first period after an emergency to reduce the effects and consequences of the emergency on people, their livelihoods, wellbeing and property; on the environment; and to meet basic human needs.
Response Agency	Any agency with a role or responsibility during an emergency response. Response agencies are either the control agency or a support agency.
Support agency	A support agency is an agency that provides services, personnel or material to support the control agency. The EMMV Part 7 – Emergency Management Agency Roles lists the support agencies for specific Class 1 emergencies and support agencies that provide specific services during all emergencies.