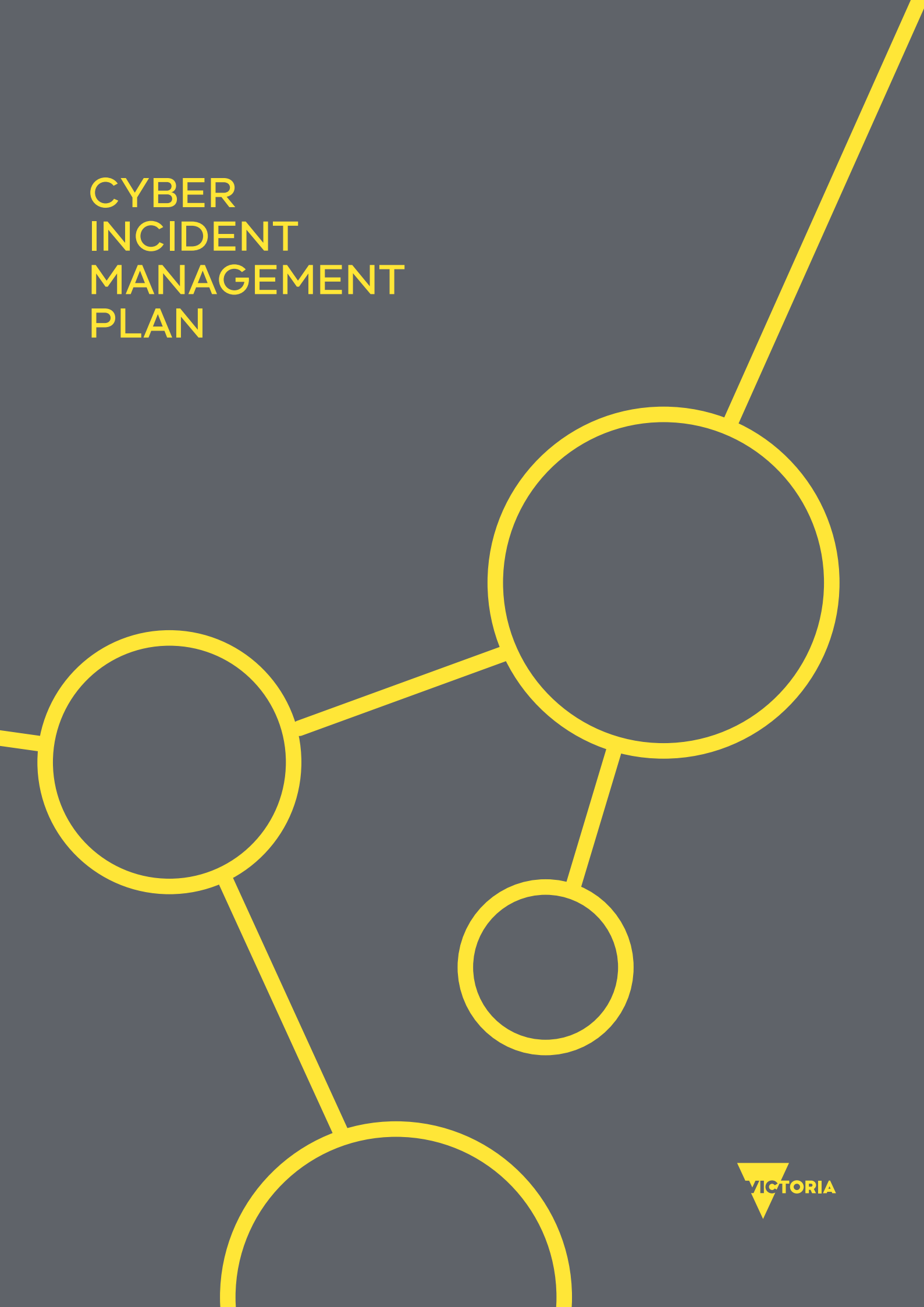
CYBER INCIDENT MANAGEMENT PLAN



VICTORIA

CONTENTS

3 Foreword

4 Introduction

7 Cyber incidents are a state significant risk

8 The Victorian Government Cyber Incident Response Service

9 Managing cyber incidents

15 Appendix A: Business Impact Level Statements

Acknowledgment

The plan was developed under the guidance of an expert working group. The Victorian Government Chief Information Security Officer extends his thanks, and acknowledges their contribution.

The working group comprised representatives of:

Cenitex
Department of Education and Training
Department of Environment, Land, Water and Planning
Department of Health and Human Services
Department of Jobs, Precincts and Regions
Department of Justice and Community Safety
Department of Premier and Cabinet
Department of Transport
Department of Treasury and Finance
VicRoads
Victoria Police

We also value the guidance provided by the Office of the Victorian Information Commissioner.

FOREWORD

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

We estimate there is an attempted compromise of Victorian Government Information Communications Technology (ICT) networks about every 45 seconds.

These attacks involve cyber criminals, nation state actors, political 'hacktivists' and online vandals.

Beyond these malicious attacks, we also face threat of human and technological error. Like with any malicious cyber-attack, the impacts of human or technological error can be significant.

Cyber incidents erode public trust in governments and impede business operations. They damage relations between jurisdictions and cause distress for community members. They also increase the risk of fraud and identity crime—especially when data breaches occur.

Responding to cyber incidents requires strong collaboration across government and industry. Organisations must be clear about their risks, roles and responsibilities. And together we must prioritise delivering the best outcomes for the community.

The Victorian Government is serious about cyber security. We have developed this plan to further improve the way we manage and respond to cyber incidents.

The plan forms part of the broader Victorian Government Cyber Incident Management Framework. It supports organisations' existing cyber incident response plans. It also connects with Victoria's emergency management and inter-jurisdictional cyber arrangements.

My vision is to make Victoria cyber safe. I want our digital systems and services to thrive in a trusted and secure cyber environment that supports all Victorians.

John O'Driscoll
Chief Information Security Officer
Victorian Government

INTRODUCTION

PURPOSE

The Victorian Government Cyber Incident Management Plan details the responsibilities of Victorian Government organisations in managing cyber incidents.

The plan supports the Victorian Government to reduce the community impacts and harm of cyber incidents.

The plan supports organisations' internal cyber incident response policies and procedures. The plan also complements Victoria's cyber emergency governance arrangements. These exist in the State Emergency Response Plan (SERP) Cyber Security Sub-Plan.

SCOPE AND AUTHORISATION

The Victorian Government Cyber Incident Management Plan is issued by the Victorian Government Chief Information Security Officer.

The plan applies to all Victorian Public Sector bodies. In this plan, these organisations are referred to as 'Victorian Government organisations'.

The plan provides important information about:

- the risk of cyber incidents to government, business and the community in Victoria
- the roles and responsibilities of Victorian Government organisations in managing cyber incidents
- the categories and terminology used by Victorian Government organisations to identify and define cyber incidents in Victoria.

Victoria's local councils are encouraged to adopt the plan.

GUIDING PRINCIPLES

The following principles underpin organisational participation in the Victorian Government Cyber Incident Management Plan.

Victoria's Government organisations will:

- remain responsive to changes in the cyber risk environment, including responding quickly to cyber incidents
- remain accountable for protecting their ICT networks against the risk of cyber incidents. This includes applying relevant regulatory controls such as the Victorian Protective Data Security Standards
- collaborate before, during and after cyber incidents to minimise potential risks to Victoria
- maintain community confidence in the ability of government to effectively manage cyber incidents.

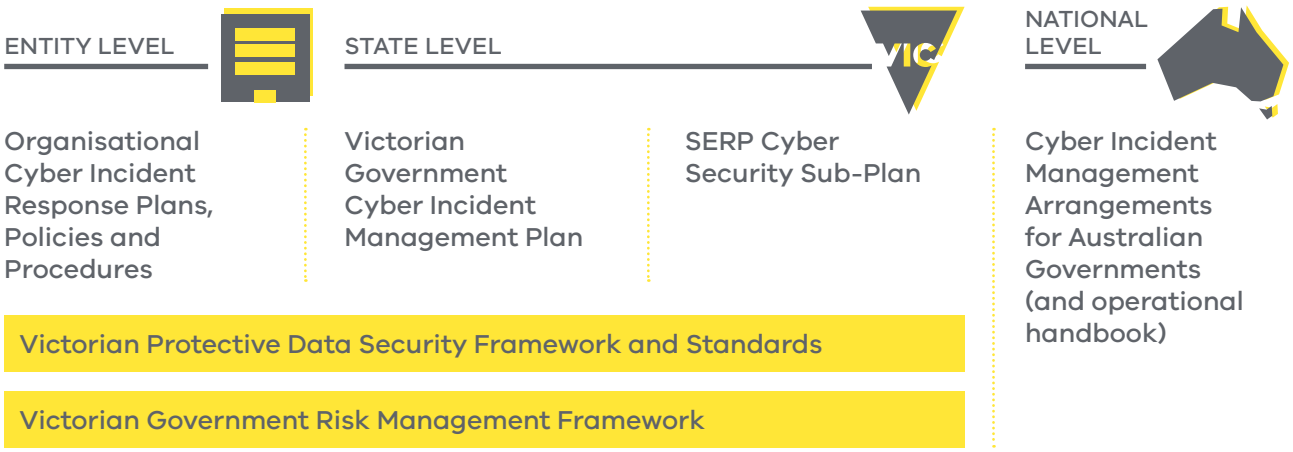
LINKAGES

The arrangements in this plan have been designed to align with the following state and federal arrangements for managing cyber incident risks:

- SERP Cyber Security Sub-Plan – the arrangements for managing cyber emergencies in Victoria
- Cyber Incident Management Arrangements for Australian Governments – the arrangements for coordinating interjurisdictional responses to national cyber incidents
- Victorian Protective Data Security Framework and Standards administered by the Office of the Victorian Information Commissioner (including the Security Incident Management Framework)
- Victorian Government Risk Management Framework.

Together, these documents form the Victorian Government Cyber Incident Management Framework.

VICTORIAN GOVERNMENT CYBER INCIDENT MANAGEMENT FRAMEWORK



REVIEW AND CONTINUOUS IMPROVEMENT

The plan will be reviewed annually by the Victorian Government Chief Information Security Officer in consultation with Victorian Government organisations.

The Victorian Government Chief Information Security Officer will establish an annual exercise to assist with reviewing the plan. Victorian Government organisations will be encouraged to participate in the exercise.

SUPPORTING VICTORIA'S PRIVATE INDUSTRY ORGANISATIONS

Victoria's private industry organisations, including community service providers and not-for-profit organisations, should contact the Australian Cyber Security Centre (ACSC) for assistance when responding to cyber incidents.

The ACSC can be contacted on 1300 CYBER1 (24/7) or via email **asd.assist@defence.gov.au**.

REDUCE THE HARM FROM CYBER INCIDENTS

We are responsive to risks

We are accountable for our networks

We always collaborate

We maintain community confidence

CYBER INCIDENTS ARE A STATE SIGNIFICANT RISK

Nine in ten Victorian Government organisations experienced a cyber incident in 2017-18. Most incidents involved 'phishing' attacks, or the discovery of malware on government ICT systems.

Three in four organisations also reported having systems or services disrupted by cyber incidents. These disruptions range from annoyances to significant system and services outages.

Some of these cyber incidents caused significant disruption to government organisations and the delivery of community services.

The cost of cyber incidents to Australia is staggering. The estimated average cost of a data breach to government organisations in Australia exceeds $1 million. More broadly, the average cost of cyber incidents to a business in Australia is around $276,000.

In addition to financial impacts, cyber incidents cause other damage including:

» damage to personal identity and reputation

» loss of business or employment opportunities

» impact on emotional and psychological wellbeing.

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

The Victorian Government treats cyber incidents as a state significant risk. We recognise the need for continued cooperation and collaboration across government to reduce the likelihood of cyber incidents occurring, and to reduce the harms they create.

THE VICTORIAN GOVERNMENT CYBER INCIDENT RESPONSE SERVICE

The Victorian Government Cyber Incident Response Service (CIRS) launched in July 2018. It was established under the Cyber Security Strategy 2016-20. The CIRS helps Victorian Government organisations respond to cyber incidents.

The CIRS sits within the Department of Premier and Cabinet. It provides organisations with access to expert cyber incident response and coordination services. This includes technical, forensics and communications specialists. These experts assist with reducing the scope, impact and severity of cyber incidents.

The CIRS is a 'second line of defence' to support Victorian Government organisations. It works with Cenitex and state/federal authorities to manage cyber incidents for the Victorian Government.

The CIRS also leads Victoria's response to cyber emergencies on behalf of the Department of Premier and Cabinet. This occurs in partnership with Victoria's emergency management authorities.

The CIRS can be contacted on 1300 CSU VIC (24/7) or cybersecurity@dpc.vic.gov.au (business hours only).

AVAILABLE SERVICES

- Threat intelligence
- Alerts and early warnings advice
- Cyber exercise support
- Incident response plan templates and guidance
- Law enforcement and national liaison
- Expert incident response and cyber forensics capabilities

MANAGING CYBER INCIDENTS

CYBER INCIDENT PREPARATION

Victorian Government organisations will

- develop and implement a cyber incident response plan for their organisation
- establish an organisational cyber incident management team that is authorised to undertake actions necessary to respond to cyber incidents
- conduct an annual exercise of the plan to identify and pursue opportunities for improvement.

Victorian Government organisations' cyber incident response plans will align with the arrangements detailed in this plan, and those detailed in the SERP Cyber Security Sub-Plan.

THREAT DETECTION AND ANALYSIS

Victorian Government organisations are accountable for identifying and managing risks to the confidentiality, integrity and availability of their digital systems, services and information.

Victorian Government organisations will analyse potential threats to determine whether a cyber incident has occurred (or is occurring). When a cyber incident is identified, Victorian Government organisations are responsible for determining the scope, impact and severity of the situation and making appropriate notifications in accordance with the advice provided in this plan.

Some Victorian Government organisations use one or more managed service providers (MSPs), such as Cenitex, to provide threat detection and analysis services. Victorian Government organisations are responsible for liaising with their respective MSPs to ensure threats are detected, analysed, communicated and managed consistent with the intent of this plan.

CYBER INCIDENT CATEGORIES

The Victorian Government uses a four-tier model for categorising cyber incidents. Cyber incidents are categorised based on the nature of the compromise and the impact(s) they create.

The four categories used by the Victorian Government are:

- Cyber Event – suspected or unsuccessful attempt to compromise with no business impact
- Cyber Incident – compromise with minor impact
- Significant Cyber Incident – compromise with limited or major impact
- Cyber Emergency – serious or exceptional compromise with community consequences.

Further guidance on cyber incident categories and notifications can be found at Table 1.

CYBER INCIDENT NOTIFICATIONS

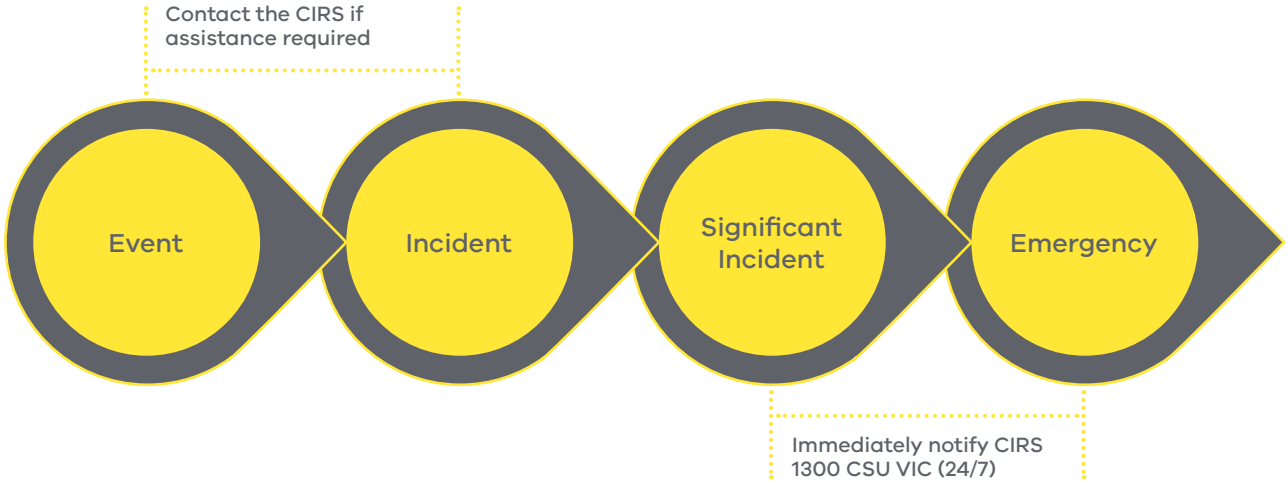
Victorian Government organisations will as soon as possible notify the CIRS of all:

» Significant Cyber Incidents

» Cyber Emergencies.

The CIRS can be contacted on 1300 CSU VIC (24/7) or via email **cybersecurity@dpc.vic.gov.au**.

Victorian Government organisations have the discretion to confirm the existence of a cyber incident before notifying the CIRS.



CIRS NOTIFICATIONS

Where the CIRS is first to identify a potential or confirmed cyber incident, the service will notify affected Victorian Government organisations, including Cenitex, as soon as possible.

CENITEX NOTIFICATIONS

Where Cenitex is first to identify a potential or confirmed cyber incident, it will notify affected organisations and the CIRS as soon as possible.

NOTIFICATIONS TO PORTFOLIO DEPARTMENTS

Victorian Government administrative offices, special bodies and public entities will notify their relevant portfolio department of cyber incidents in a timely manner. This is to support the establishment of collaborative response efforts.

Portfolio departments will provide administrative offices, special bodies and public entities with guidance on notification arrangements, where these arrangements do not already exist.

ADDITIONAL NOTIFICATIONS

Victorian Government organisations should also notify the Office of the Victorian Information Commissioner and the Victorian Managed Insurance Authority (or their alternative cyber insurance provider) of cyber incidents.

Victorian Government organisations should consider their legal obligations when determining the full scope of cyber incident notification requirements.

If a cyber-incident involves unauthorised access to or loss of personal information, and there is a risk of harm to the people the information is about, Victorian Government organisations should consider notifying those people of the cyber incident.

Further information can be found in the Office of the Victorian Information Commissioner's guide to '**Managing the Privacy Impacts of a Data Breach**'.

TABLE 1: CYBER INCIDENT CATEGORIES

See Appendix A for the detailed business impact level statements.

Category and Business Impact Level	Description and Impact Statement	Notification Requirements	Triggers for escalating to higher category
Cyber Event Business Impact Level 0	A suspected (or unconfirmed) cyber incident with no impact to systems or services.	Consider notification to internal security representative.	Substantial increase in cyber security alerts; or continued cyber security alerts with potential to breach security controls.
Cyber Incident Business Impact Level 1	Successful compromise of security controls. Minor impact to services, information, assets, reputation or relationships.	Contact the CIRS if assistance is required to respond to the incident. Contact 1300 CSU VIC (24/7) cybersecurity@dpc.vic.gov.au.	Actual or high likelihood: › for limited or major impact to services; or › to affect multiple organisations; or › data breach
Significant Cyber Incident Business Impact Levels 2 and 3	Successful compromise of security controls. Limited or major impact to services, information, assets, government reputation, relationships and/or the community (but not an emergency). A significant cyber incident is also any cyber incident that involves: › critical infrastructure or essential services; or › more than one organisation; or › a data breach.	Victorian government organisations will immediately notify the CIRS of all significant cyber incidents. Contact 1300 CSU VIC (24/7) cybersecurity@dpc.vic.gov.au.	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 Emergency Business Impact Levels 4 and 5	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.	Immediately contact 1300 CSU VIC (24/7) The Department of Premier and Cabinet is Victoria's lead department for responding to cyber emergencies. Immediately notify the CIRS and apply organisational emergency management arrangements in consultation with DPC and Emergency Management Victoria.	N/A

TECHNICAL RESPONSE ACTIVITIES

Single organisation cyber incidents

Victorian Government organisations are responsible for undertaking any technical activities necessary to respond to cyber incidents. These services may be provided by a MSP, including Cenitex, where third-party assistance is required.

Victorian Government organisations may also request technical assistance from the CIRS if help is required.

Multi-organisation cyber incidents

The CIRS is responsible for managing Victorian Government responses to multi-organisation cyber incidents. This responsibility is identified in the Cyber Security Strategy 2016-20.

This includes responding to cyber incidents affecting MSPs and contracted /shared service providers used by multiple Victorian Government organisations.

The CIRS will collaborate with all affected Victorian Government organisations to provide effective leadership and coordination of cyber incident response activities.

INTELLIGENCE SHARING

The CIRS is responsible for managing the flow of cyber risk intelligence across Victorian Government organisations. This includes:

- Gathering and sharing technical information about cyber incidents to inform Victorian Government response efforts, including liaison with the Australian Cyber Security Centre.
- Developing a whole-of-government picture of cyber incidents to inform organisations, government and other stakeholders (including the media and public).

Victorian Government organisations are responsible for sharing information and intelligence with the CIRS to support this objective.

EMERGENCY MANAGEMENT LIAISON

If a cyber incident causes, or is likely to cause, a genuine threat to health and safety, damage to Victoria's environment or significant adverse community consequences, the situation may escalate to a cyber emergency.

All cyber emergencies must be immediately reported to the CIRS on 1300 CSU VIC.

The Department of Premier and Cabinet is Victoria's lead department for responding to cyber emergencies. The department works closely with Emergency Management Victoria and Victoria's emergency management sector to manage cyber emergencies.

The SERP Cyber Security Sub-Plan details Victoria's arrangements for responding to cyber security emergencies. It provides information about response coordination, control, command, communications and consequence management activities.

POLICE LIAISON

The CIRS works closely with Victoria Police to share information and intelligence about cyber incidents affecting the Victorian Government.

The CIRS will refer to Victoria Police all cyber incidents that are suspected criminal offences.

Victorian Government organisations may also refer cyber incidents directly to Victoria Police, or via the national **Cyber Issue Reporting System**

NATIONAL LIAISON

The interconnected nature of our digital world means that some cyber incidents can affect multiple Australian states and territories simultaneously. This was observed during the 2017 'Wannacry' ransomware incident that disrupted several thousand computer devices worldwide.

In 2018, Australian state and territory governments and the Commonwealth developed the Cyber Incident Management Arrangements for Australian Governments.

The arrangements outline the principles and inter-jurisdictional coordination arrangements for Australian governments' cooperation in response to national cyber incidents.

The Victorian Government Chief Information Security Officer is Victoria's representative to other Australian governments during a national cyber incident, as a member of the National Cyber Security Committee.

The National Cyber Security Committee comprises government cyber security leads from all Australian states and territories and the Commonwealth Government.

It is responsible for supporting national coordination and increased situational awareness during national cyber incidents.

MEDIA AND PUBLIC COMMUNICATIONS

It is important to provide media and the public with information about cyber incidents that affect the delivery of government services, or which may cause harm to the community.

Single organisation cyber incidents

Victorian Government organisations are responsible for managing media and public communications about cyber incidents.

Subject to the circumstances of an incident, media and public communications should ideally provide information about:

- the nature and impact of a cyber incident
- the extent of affected systems/services
- the steps being taken to resolve the cyber incident
- when systems/services are expected to return to operation (if known)
- any other information relevant to minimising the harm of the cyber incident.

Any Victorian Government organisation that requires assistance with media and public communications during a cyber incident can contact the CIRS.

Multi-organisation cyber incidents

During multi-organisation incidents the CIRS will coordinate media and public communications in conjunction with impacted organisations' media and communications staff.

The CIRS will also liaise with the Australian Cyber Security Centre and members of the National Cyber Security Committee. These groups will share key messages about cyber incidents to support consistent media and public communications across jurisdictions.

If the impacts of a cyber incident are isolated to a specific industry or sector, responsibility for managing media and public communications may be transferred to the relevant portfolio department or agencies.

MINISTERIAL ENGAGEMENT

Victorian Government organisations are responsible for briefing their respective Minister(s) in relation to cyber incidents.

During multi-organisation cyber incidents, the CIRS will prepare and circulate communications to support organisations in delivering consistent briefings to Ministers.

CYBER INCIDENT RECOVERY

Cyber incidents can damage important ICT assets (including hardware and data) and other infrastructure, disrupting the delivery of business and community services.

It is important that Victorian Government organisations develop, implement and regularly practice their business continuity and ICT disaster recovery arrangements.

This will assist with returning impacted systems and services to normal operation as soon as possible.

APPENDIX A: BUSINESS IMPACT LEVEL STATEMENTS[1]

Business Impact Level	Descriptor	Key Indicators and Consequences for Cyber Incidents
N/A Business Impact Level 0	**No** business impact	› No service impact
Minor Business Impact Level 1	Compromise of the information would be expected to cause **Minor** harm/damage to government operations, organisations or individual	› Compromise of an organisation's non-critical (non-essential) physical or material assets › No threat to, or disruption of business operations, systems or service delivery › No damage to relations between Victorian Government and other governments
Limited Business Impact Level 2	Compromise of the information would be expected to cause **limited** harm/damage to government operations, organisations or individuals	› Reputational damage or embarrassment for the organisation › Public concern or dissatisfaction › Degradation or cessation of non-critical (non-essential) business operations, systems or services, leading to reduction in the efficiency and effectiveness of functions
Major Business Impact Level 3	Compromise of the information would be expected to cause **major** harm/damage to government operations, organisations or individuals	› Reputational damage or embarrassment for the organisation › Broad public concern or dissatisfaction › Degradation or cessation of critical (essential or important) business operations, systems or services, to an extent that the organisation cannot perform one or more of its primary functions › Breach of personal information (including sensitive information as defined in Schedule 1 of the PDP Act 2014)
Serious Business Impact Level 4	Compromise of the information would be expected to cause **serious** harm/damage to government operations, organisations or individuals	› Reputational damage or embarrassment for the organisation and /or the government of the day › Widespread public concern or dissatisfaction › Degradation or cessation of critical (essential or important) business operations, systems or services, to an extent that the organisation cannot any of its functions
Exceptional Business Impact Level 5	Compromise of the information would be expected to cause exceptionally grave damage to the national interest	› Refer to the Commonwealth Protective Security Policy Framework (PSPF)

1 Based on the Office of the Victorian Information Commissioner, Victorian Protective Data Security Framework Business Impact Levels, Version 2.0, February 2019.

VICTORIAN GOVERNMENT CYBER INCIDENT MANAGEMENT PLAN

Content coordination

Enterprise Solutions Branch, Department of Premier and Cabinet

Design by Claire Ho Design

All images by iStock

Accessibility

If you would like to receive this publication in an accessible format, please contact the department on 9651 5111

Information in this document is available on vic.gov.au

ISBN 978-1-925789-27-0 (pdf/online/MS word)

Authorised and published by the Victorian Government
1 Treasury Place, Melbourne 3002

Disclaimer

This publication may be of assistance to you but the State of Victoria and its employees do not guarantee that the publication is without flaw of any kind or is wholly appropriate for your particular purposes and therefore disclaims all liability for any error, loss or other consequence which may arise from you relying on any information in this publication.

VICTORIA