ICT Network and Cyber Security Statement of Direction

for the Victorian Public Service

August 2016

VICTORIA State Government | Premier and Cabinet

Contents

Vision and purpose

VISION	A consistent and managed data network for the Victorian Government that enables secure shared ICT services and employee productivity. Consistent and coordinated cyber security planning and services.		
PURPOSE	Increase the interconnectivity, security, reliability and accessibility of departmental and shared services over a data network that is managed with an understanding that it is part of the Victorian Government as a whole. Uplift cyber security capability to preserve business continuity for the Victorian Government, resilience of government services and the protection of sensitive data against loss, malicious alteration and unauthorised use.		
APPLIES TO	All Departments, Victoria Police, CenITex	**AUTHORITY**	Victorian Secretaries Board
PERIOD	2016 to 2020	**ADVISED BY**	DPC, following consultation with the CIO Leadership Group
ISSUE DATE	August 2016	**DOCUMENT ID**	SOD/ NetworkCyberSec/01 TRIM DPC D16/123639
REVIEW DATE	August 2019	**VERSION**	1.0

Introduction

The *Victorian Government ICT Network and Cyber Security Statement of Direction* sets out the high-level requirements for the government's ICT network and improved cyber security capabilities. The ICT network will address connectivity issues between existing Victorian Government ICT networks to:

- improve productivity
- reduce network management costs
- support secure data exchange
- improve network data security and cyber resilience
- facilitate government workplace objectives.

Background and context

The Victorian Government uses information and communication technology (ICT) across government departments, agencies and employees. ICT supports the operation of the government, allowing it make decisions and deliver services to Victorians.

Over time, government ICT networks and related services have become disparate, with some departments and agencies (hereafter: "departments") managing their own separate ICT networks, resulting in gaps in connectivity across government. This lack of connectivity affects each department's capability to deliver services efficiently and effectively, particularly when cross-government information sharing is needed.

The workplace environment described in the *Workplace Environment Statement of Direction* issued by DPC in 2015 requires an uplift in network capability.

The security of government information is of significant importance, and the need for improvement has been highlighted by successive information security-related reports from the Victorian Auditor-General and the Commissioner for Privacy and Data Protection.

The *Information Technology Strategy, Victorian Government, 2016 to 2020* (the *Strategy*) sets strategic objectives for the Victorian Government, including a recognition of the current and emerging cyber threat landscape.

The *Strategy* and the Commonwealth report *Australia's Cyber Security Strategy* provide the context and background that recognises the Victorian Government should:

- uplift its cyber security capability to preserve business continuity for government
- improve the resilience of government services
- increase the protection of data against loss, malicious alteration and unauthorised use.

Victoria's Commissioner for Privacy and Data Protection has issued the *Victorian Protective Data Security Framework* which is the "overall scheme for managing protective data security risks in Victoria's public sector".

Context Documents

- *Australia's Cyber Security Strategy*, Commonwealth Government, 2016
- *Information Technology Strategy, Victorian Government, 2016 to 2020,* DPC, Victorian Government, 2016
- *Workplace Environment Statement of Direction* (STD/Workplace/01) DPC, Victorian Government, 2015
- *Victorian Protective Data Security Framework* (VPDSF) Commissioner for Privacy and Data Protection, Victorian Government, 2016

Scope

The following departments and agencies are formally in scope:

- Department of Economic Development, Jobs, Transport and Resources
- Department of Education and Training
- Department of Environment, Land, Water and Planning
- Department of Health and Human Services
- Department of Justice and Regulation
- Department of Premier and Cabinet
- Department of Treasury and Finance
- Victoria Police
- CenITex

Key objectives

This section addresses the key objectives for the two parts of this statement of direction: network and cyber security.

Network

Objective

Leverage existing and create new components to establish a Victorian Government core ICT Network – the "Victorian Government Network" (VGN) to:

- provide coordinated and centralised network management and common services catalogue items
- implement a single Victorian Government identity and related identity and access management services as defined in the *Workplace Environment Statement of Direction* (SOD/Workplace/01)
- provide network zones for portfolio-based data requiring higher levels of protection
- align with Victorian Government network security standards, supporting a consistent level of trust and data protection
- provide a platform that facilitates the delivery of government objectives including collaboration tools, 'app' store and document management in line with the previously released *Workplace Environment Statement of Direction*.

Cyber security

Objective

Develop stronger cyber security defences to:

- strengthen government ICT networks and systems to provide increased resilience from attack and compromise
- increase detection, deterrence and response to cyber security threats and events
- enable better understanding and monitoring of risks.

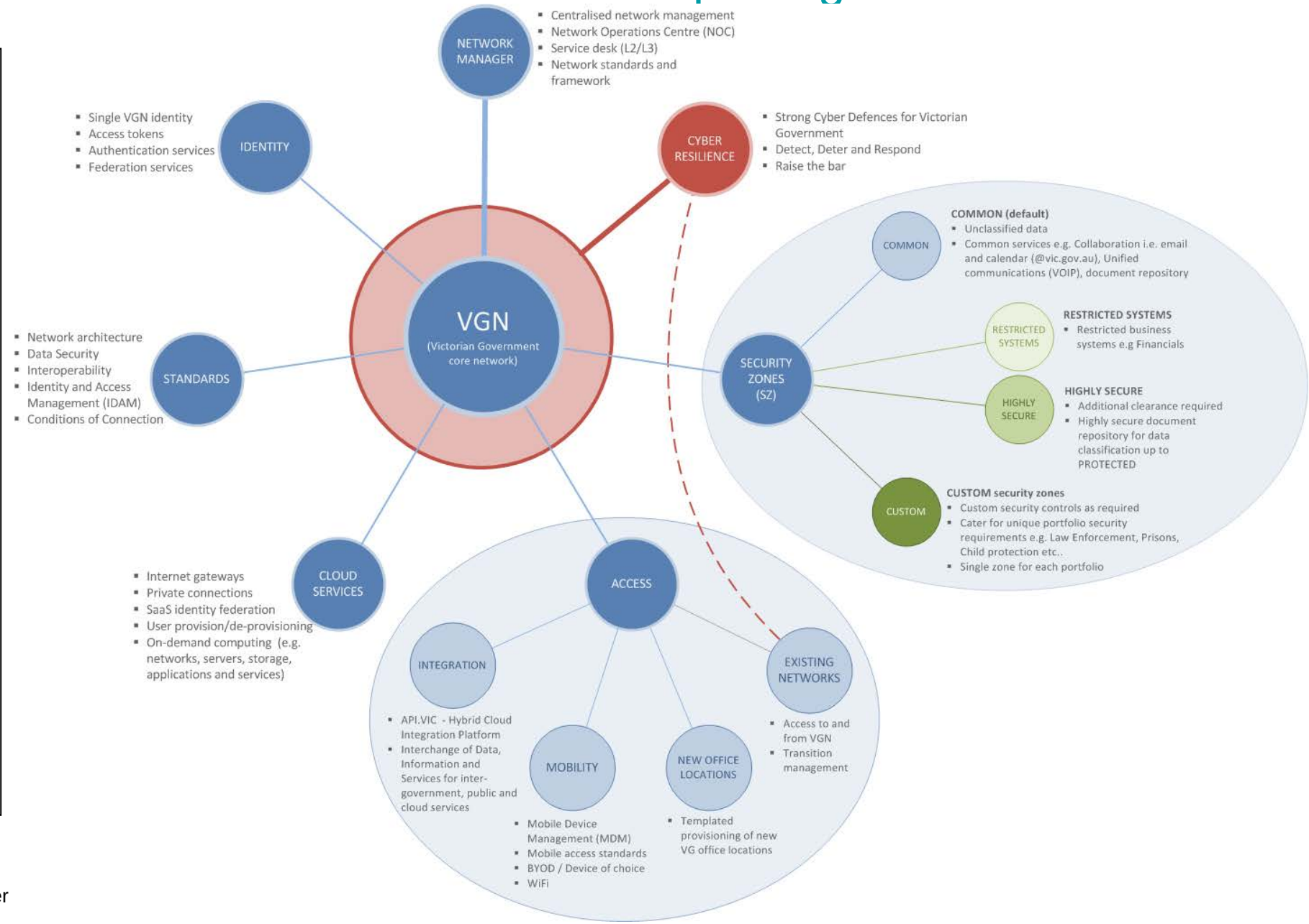
How does this statement of direction help the government?

The VGN provides the government with the benefits of interconnectivity and improved security across connected departments and agencies.

Network standardisation supports consolidation efforts and enables a reduction of network costs.

Strong cyber defences uplift the resilience of ICT networks and systems from attack.

This diagram sets the VGN and cyber resilience in the broader context of government ICT systems and other current and proposed Statements of Direction.



Direction

Network

The following section outlines the high level requirements for the VGN.

There are six categories of requirements for the VGN:

1. network manager
2. identity
3. standards
4. security zones
5. access
6. cloud services.

Network manager

Objective

Provide coordinated and centralised network management of the VGN and offer a range of high quality, value for money, services catalogue items to departments and agencies.

Reference	Direction	Benefit to government
VGN-01	The VGN will have a single network manager.	The network manager will provide coordinated and centralised network management of the VGN. It will offer a range of high quality, value for money, common services items to departments and agencies. **Note**: some departments currently operate their own networks. This Statement notes a direction for consolidated management, but this will be the subject of separate business case and procurement decisions.
VGN-02	The network manager will provide a range of services for the VGN and its connected environment, including: ▪ core network management ▪ network operations centre (NOC) ▪ network design standards and framework ▪ perimeter management ▪ interconnects ▪ LAN management ▪ L2/L3 service desk ▪ transition management ▪ Security Operations Centre (SOC) integration and operational support.	An example of the type of services in each service category is listed in Appendix A – network manager. The SOC is also noted within the cyber security section of this Statement of Direction.

Identity

Objective

Implement the single Victorian Government identity (ID) and related identity services as defined in the *Workplace Environment Statement of Direction* (SOD/Workplace/01).

Reference	Direction	Benefit to government
VGN-03	The VGN will implement the common Victorian Government network logon/username requirement as defined in the *Workplace Environment Statement of Direction*, reference ID-03/04.	▪ Increased productivity via a single logon/username to access all services provided through the VGN. ▪ Improved security by removing redundant credentials. For information: *Workplace Environment Statement of Direction* extracts: **ID-03:** Common Victorian Government network logon/username ▪ One logon/username that is same as or linked to the staff ID. ▪ Username can be associated with a password, token or smartcard for authentication to the common VG network and related services **ID-04:** Access to common systems ▪ One username can be used to access the App Store for requesting, installing and running applications – refer to App Store. ▪ Allows for single-sign-on – using the one username to access multiple systems without the need to re-authenticate (application dependent). ▪ Allows for same-sign-on – use the one username to access multiple systems with the same credentials (requires re-logon). ▪ This username can be used to: o access collaboration systems and tools – refer to collaboration o access and assign file/folder permissions to the common document management system – refer to document management o access the hot desk environment – refer to office productivity o access the virtual desk environment – refer to devices.

VGN-04	The VGN will accommodate the common Victorian Government staff ID requirement as defined in the *Workplace Environment Statement of Direction*, reference ID-01.	▪ Every user account will be associated/linked to the staff ID, clearly showing who is accessing services hosted in and provided by the VGN. For information: *Workplace Environment Statement of Direction* extract: **ID-01:** Common Victorian Government network staff ID ▪ One unique Victorian Government ID. ▪ The ID stays the same regardless of changes as a result of MoG, marital status, gender, employment type or even gaps in employment (i.e. returning to Victorian Government).
VGN-05	The VGN will provide identity federation services.	▪ Identity federation will be used by external systems, including cloud identity services, to provide a 'single-sign-on' user experience. ▪ Identity federation improves security by never storing user passwords outside of the VGN, as is the case with many cloud systems. ▪ Identity federation reduces the number of user accounts (username and password) by consolidating all external access into the one fully managed and auditable logon. ▪ Identity federation improves provisioning and de-provisioning efficiency through the reduction of user accounts.

Standards

Objective

The VGN will conform to existing Victorian Government security and information management standards and where applicable develop, maintain and implement network standards and frameworks based on industry best practice.

Reference	Direction	Benefit to government
VGN-06	The VGN will conform to all Victorian Government security and information management standards.	▪ Security and information management compliance. ▪ Conforming to standards will form part of the network manager's (VGN-02) key performance indicators.
VGN-07	The network manager will develop VGN standards and frameworks based on current industry best practice.	▪ A standards approach will maximise: o reliability, maintainability and longevity o security and information management compliance o user/customer experience. ▪ Standardisation across the VGN and existing agency networks supports consolidation and reduces network costs.

Security zones

Objective

Provide network zones/enclaves for data that requires higher levels of protection.

Reference	Direction	Benefit to government
VGN-08	The VGN will provide a default or COMMON zone for unclassified data and common systems.	▪ Services in the COMMON zone are not bound to particular departments and therefore will not be affected by machinery-of-government changes. ▪ The COMMON zone will allow easier collaboration as it hosts common unclassified systems and data for all users (with access). ▪ Supports corporate systems including email (@vic.gov.au), calendar, unified communications, and common document repository.
VGN-09	The VGN will contain security zones or enclaves.	▪ The VGN will contain a number of default security zones or enclaves that cater for incremental higher security requirements. ▪ Additional security controls zones can be customised to meet unique security or services requirements for a given system or portfolio, e.g. law enforcement, emergency services or child protection.
VGN-10	The VGN will provide two additional zones for data higher than 'unclassified': ▪ RESTRICTED SYSTEM ▪ HIGHLY SECURE.	▪ These additional security zones provide a starting point for data requirements higher than 'unclassified'. ▪ **RESTRICTED SYSTEMS** o This enclave provides a hosting environment for business systems that have restricted access, e.g. human resources. o Access to this zone will be granted to users that require access to hosted business systems as part of their job description. o No additional security clearance is required for this zone. ▪ **HIGHLY SECURE** o This enclave hosts a highly sensitive document repository for Victorian Government (all departments) for data classification up to PROTECTED. o Additional security clearance is required to gain access to this zone.
VGN-11	The VGN will allow for the creation of CUSTOM zones.	▪ The CUSTOM zone will cater for unique portfolio security or service requirements, e.g. law enforcement, emergency services, prisons or child protection. ▪ Each portfolio will have a single zone with custom security controls and conditions of access determined by the portfolio owner. ▪ There is no restriction on the services that can be made available in a custom zone. ▪ Portfolio-based custom zones are not bound to particular departments or agencies and therefore will not be affected by machinery-of-government changes.

Access

Objective

Provide access to the VGN and related services, including from:

- existing agency networks
- newly provisioned office locations
- mobile devices.

Reference	Direction	Benefit to government
VGN-12	The VGN will allow access from existing agency networks.	▪ Existing agencies will have access to the VGN and related services from their existing networks. ▪ It is expected that all **department** networks will, over time, be consolidated into the VGN. ▪ Connectivity to the VGN will be available for external agency networks (currently not in scope). This will allow them to benefit from the services of the VGN, including the Security Operations Centre (SOC).
VGN-13	The VGN will implement the all-access (network access) requirements as defined in the *Workplace Environment Statement of Direction*.	▪ The VGN will provide methods of access that a user expects from a modern workplace environment. See extract: **NA-01:** A user will have access to a common Victorian Government (VG) network ▪ New workplace services and select existing services will be accessible via a common VG network **The following requirements are an extension to the common network environment listed in NA-01.** **NA-02:** Logon using a Victorian Government username ▪ Access to the VG network will be authenticated using the VG username **NA-03:** From multiple devices and locations ▪ Access to the VG network will be available from any corporate and approved BYOD device at any VG location via cable or WiFi. ▪ Remote (offsite) access to the network will be available for any corporate and approved BYOD device via the internet. ▪ Note – remote access will require additional security and/or authentication **NA-04:** Network performance ▪ 'Fast/consistent network speed': o low latency from all VG office locations including regional offices. o minimal impact on desktop logon/off times for all corporate provide devices o responsive access to all workplace services.

Cloud services

Objective

Provide connectivity to a range of cloud services from the VGN.

Reference	Direction	Benefit to government
VGN-14	The VGN will implement a hybrid cloud integration platform.	▪ An integration platform will provide secure connectivity for the interchange of data, information and services: ▪ across government on-premise systems and cloud services, cloud systems, and agency systems (agency to agency including Service Victoria). ▪ for public source data for data.vic, and for API public consumption, e.g. mobile. ▪ An integration platform removes the need to implement 'point to point' solutions. This de-coupling of systems improves flexibility (change without impact) and reduces system integration complexity and associated costs.
VGN-15	Access to the internet from within the VGN will only be permitted from VGN-enabled internet gateway(s).	▪ The VGN internet gateway(s) will provide enhanced protection through an end-to-end service from defined and clearly managed connection points. ▪ All VGN internet gateways will be monitored by the approved government security operations centre service (SOC).
VGN-16	The VGN will provide identity federation for use by cloud services.	▪ Identity federation (refer Identity, VGN-05) enables cloud services to use the VGN identity for authentication, improving security and removing the need for multiple user accounts.
VGN-17	Private connections to cloud services will be managed by the network manager.	▪ Connection to third-party systems outside of the VGN will be assessed and managed by the network manager, ensuring access and security standards and maintained.
VGN-18	The VGN will offer a range of on-demand computing services as part of the network manager's catalogue items.	▪ On-demand computing managed through the network manager provides rapid delivery without compromising security. ▪ On-demand computing includes networking, servers, storage, applications and services.

Cyber security

Resilience

Objective

Improve the maturity of government's cyber security resilience capabilities.

Reference	Direction	Benefit to government
VGN-19	The Victorian Government will have a cyber security strategy.	The *Cyber Security Strategy* will: ▪ improve governance and accountability arrangements ▪ increase the level of coordination across government ▪ improve the information flow for security alerts and sharing of incident data ▪ describe the new cyber security capabilities required to respond to the threat landscape, including the Security Operations Centre Service (SOC).
VGN-20	The Victorian Government will have a cyber resilience framework.	The cyber resilience framework has four objectives: ▪ provide cyber security governance, including an effective framework for monitoring cyber activities, partner collaboration opportunities and a process for managing cyber security risks and obligations ▪ cyber security situational awareness, which will provide a process for gathering, analysing and sharing cyber intelligence and assess options for developing a proactive security intelligence network across government ▪ cyber resilience assessment, which will provide a baseline understanding of government's current cyber resilience levels and an ongoing process for the assessment and identification of departmental needs for continued cyber security improvements cyber response plan, which will outline the necessary cyber security programs to increase capability to prevent, detect and respond to cyber security incidents, and minimise the impacts of these incidents
VGN-21	The Victorian Government will have a Security Operations Centre (SOC) service.	The government SOC will deliver: ▪ a shared services model for the delivery of government cyber security services ▪ coordinated and timely responses for all cyber security threats and alerts ▪ access to industry specialists for forensic analysis and threat and vulnerability identification ▪ a managed security services panel, to support departments with access to prequalified security providers across services categories.

Implementation

Implementation of the elements of this *Statement* will align with the *IT Strategy's* governance and implementation structure of shared services in the Victorian Government. DPC will work with relevant stakeholder groups to determine opportunities for design and implementation.

Document control

Approval

This Statement of Direction was approved by the Victorian Secretaries Board on 17 August 2016 and applies from the date of issue (see cover).

Version history

Version	Date	Comments
0.1	January 2016	Initial framework draft
0.2	March 2016	Updates based on initial feedback from A/g ED ESB
0.4	March 2016	Versioned for CIO Leadership review and discussion at meeting on 11 March 2016
0.7	April 2016	Integration added and implementation section updated. Change from 'Requirement' to 'Direction' (table header)
0.8	April 2016	Change SECURE/CABINET zone definition to HIGHLY SECURE due to ongoing discussion around CABINET classification with DPC and CPDP
0.9.1	May 2016	Renamed and updated to include Cyber Security; Information Security Advisory Group contributions.
0.9.2	May 2016	Minor changes based on internal review. Version distributed to CIO leadership group and CenITex for final review
0.9.3	June 2016	CIO Leadership Group review.
0.10	June 2016	Updates from 0.9.2 based on A/g Exec Director, Enterprise Solutions review.
0.11	June 2016	Internal ESB review
0.12	June 2016	Draft for CIO Leadership Group and CenITex final review and distribution
1.0	August 2016	Final for VSB consideration/approval (also sent to CIO Leadership Group)

Glossary

Term	Meaning
CPDP	The Office of the Commissioner for Privacy and Data Protection https://www.cpdp.vic.gov.au/
Cyber resilience	Cyber resilience is the organisation's capability to withstand negative impacts due to known, predictable, unknown, unpredictable, uncertain and unexpected threats from activities in cyberspace (ISF 2011). The ideal situation is one where the organisation minimises its cost of controls, responses and other cyber resilience activities, relative to the expenditure needed to minimise the cost of negative impacts from activities in cyberspace (ISF 2011).
ICT Network	Means for the exchange of data between computers.
IT Strategy	*Information Technology Strategy for the Victorian Government, 2016 to 2020*
IDAM	Identity and Access Management
MoG changes	Machinery of government changes
Protective marking	A protective marking indicates the required level of protection to all users of the information. There are three types of protective markings: security classifications, dissemination limiting markers (DLMs) and caveats. Refer to the information security management guidelines - Australian Government security classification system. https://www.protectivesecurity.gov.au/informationsecurity/Pages/AustralianGovernmentSecurityClassificationSystem.aspx
public entities	Refer to Victorian Public Entities
public service body	Refer to Victorian Public Service
security classification	Security classifications reflect the level of damage done to the state/national interest, organisations and individuals of unauthorised disclosure, or compromise of the confidentiality.
SOC	Security Operations Centre
SOD	Statement of Direction
Victorian Public Entities	The definition of a public entity is comprehensive and will not be reproduced here. For a full definition, please refer to the *Public Administration Act 2004.*
Victorian Public Sector	The Victorian Public Sector comprises the Victorian Public Service and Victorian Public Entities – refer to the *Public Administration Act 2004.*
Victorian Public Service	The Victorian Public Service, also referred to as public service bodies, means a) Departments, b) an Administrative Office; or (c) the State Services Authority - refer to the *Public Administration Act 2004.*
VPDSS	*Victorian Protective Data Security Standards* published by CPDP www.cpdp.vic.gov.au/menu-data-security/victorian-protective-data-security-framework/vpdsf
VSB	Victorian Secretaries Board
Workplace Environment	*Workplace Environment Statement of Direction* (SOD/Workplace/01) www.vic.gov.au/digital-strategy-transformation-statements-direction

Appendix A

Network manager

The following table provides additional detail of the services for the network manager. The scope of services are non-exhaustive and considered a starting point for the type of services in each service category.

Service category	Scope of services for government
Core network management	▪ Design, implement and maintain the VGN. ▪ Manage core network operations, including network monitoring and perimeter management (refer Perimeter Management service category). ▪ Deploy cybersecurity monitoring tools that meet and support Victorian Government standards and policies. ▪ Provide connectivity to the Victorian Government Security Operations Centre (SOC) ▪ Implement and maintain VGN security zones (refer security zones section) ▪ Provisioning of interconnects between service provider gateways and VGN (refer Perimeter Interconnects service category) ▪ Support network design to accommodate new services e.g. IP-telephony, Unified Communications (UC), multimedia communication ▪ Provisioning of network connectivity for enablement of cloud services including but not limited to Data Centre as a Service, Platform as a Service, Identity as a Service and Software as a Service. ▪ Wi-Fi enablement and rollout (also refer Access section) ▪ IP address management including IPv6 transition plan as required. ▪ Manage customer quality of service (QoS) across networks ▪ Break/fix for managed network equipment (including field operations) and management of vendors for warranty and spares for network equipment

Network Operations Centre (NOC)	▪ Network monitoring and control services include, but not limited to:
	  ▪ Network monitoring
	  ▪ Incident/outage response
	  ▪ Incident reporting
	  ▪ Custom service monitoring

Network design standards and framework	▪ Design and maintain:
	  ▪ Network architecture and standards
	  ▪ Wi-Fi architecture and standards
	  ▪ Interoperability (in multi-vendor environments) standards
	▪ Conform to existing Victorian Government standards in relation to;
	  ▪ Information management
	  ▪ Security
	  ▪ Identity
	  ▪ new policies and standards as required
	▪ Conditions of Connection

Perimeter management	▪ Perimeter network management which includes:
	  ▪ Internet gateways
	  ▪ Web servers, mail servers, FTP servers
	  ▪ Other network-access control devices

Interconnects	▪ Facilitate and manage network interconnects to and from the government core network edge devices and other networks, including the last POI (point of interconnection) the core network and cloud service providers, in addition to tail-end carriers.

LAN management	▪ LAN management including, but not limited to:
	  ▪ Network discovery, topology views, end-station tracking, and VLAN management
	  ▪ Real-time network fault analysis with easy-to-deploy, device-specific, leading practice templates
	  ▪ Hardware and software inventory management, centralised configuration tools, and syslog monitoring
	  ▪ Monitoring and tracking of network response time and availability
	  ▪ Real-time device and link management, as well as port traffic management, analysis, and reporting

L2/L3 service desk	▪ Level 2 and 3 technical support and troubleshooting of network services ▪ Provision of a service desk and fault resolution service capable of managing multiple vendors ▪ Single point of contact for network issue reporting, resolution and escalation for services delivered by third party suppliers ▪ Requires integration with managed Level 1 Service Desk Services as currently utilised by agencies (where applicable)

Transition management	▪ Technical and operational transition of network services for agencies, this may include services transitioned from:
	  ▪ Department and agency current managed services
	  ▪ Services currently managed by third party suppliers.
	▪ Network transition services which may include:
	  ▪ Managed routers and switches
	  ▪ Security monitoring
	  ▪ Management of perimeter security and DMZs
	  ▪ ISDN circuits to SIP trunking
	  ▪ Private clouds
	  ▪ LAN management
	▪ Management of the transition of environments with multiple carriage providers and technology service offerings

Security Operations Centre (SOC) integration and operational support	▪ Facilitate and manage VGN connectivity to the Security Operations Centre (SOC) ▪ Assist external agency networks connectivity to the VGN SOC ▪ Assist SOC as required during incident response, diagnostics and Isolation