Asset Management Plan

IT – Infrastructure

Version Number: 2.1

Date: January 2023

Document Control

Authorisation

Action	Name and title	Date	Signature
Prepared by		22/2/2022	
Reviewed by		16/1/2023	
Authorised by		16/1/2023	
Review cycle	5 Years from date of last approval		

Contact

This document is the responsibility of the Information Technology Group, Tasmanian Networks Pty Ltd, ABN 24 167 357 299 (hereafter referred to as "TasNetworks").

Please contact the Leader Information Technology with any queries or suggestions.

Responsibilities:

Implementation	All TasNetworks staff and contractors.
Compliance	All group managers.

Revision

Date	Version	Description	Author	Approved by
15/06/2017	0.8	Review Version		
26/10/2017	0.9	Update comments from Leader IT		
27/10/2017	1.0	Approved Version		
03/09/2021	1.9	Draft R24 Update		
24/2/2022	2.0	R24 Approved Version		
16/01/2023	2.1	Minor revisions		

Copyright

Table of Contents

1 Background and Purpose

The TasNetworks Information Technology team is responsible for delivering architecture, infrastructure, application and desktop services to TasNetworks corporate and network operations customers. IT Infrastructure systems are the shared hardware, software, monitoring and administration tools forming the foundation of shared IT capabilities upon which business systems are built.

This Asset Management Plan details TasNetworks' plan for IT Infrastructure System assets for the 5 year period 2024 – 2029. The strategies outlined in this plan have been developed taking into account past asset performance, industry best practice and the need for prudent investment to optimise the asset lifecycle costs and performance.

The objective of this plan is to minimise business risk to within acceptable limits – utilising the TasNetworks risk framework and achieving reliable asset performance at an optimal lifecycle cost. The replacement program outlined will mitigate business risks presented by each asset category and optimise the economic life of each asset according to the important factors of capability, obsolescence and the increasing emergence of cyber security threats. These factors are relatively important when dealing with such complex technology, compared to wear and tear.

This plan supports the TasNetworks business and technology by providing effective and efficient solutions while rationalising the IT environment and reducing costs while enabling delivery of new business application services to support TasNetworks corporate objectives.

2 Scope

2.1 In Scope

This asset management plan covers the identification, procurement, implementation, maintenance and disposal of all IT Infrastructure systems within TasNetworks. IT Infrastructure systems include the following:

IES Category / Service	Service Subclass	Typical Products
Application Delivery	Application Deployment Application Patching Application Platforms Application Virtualisation	[redacted]
Collaboration	Conferencing E-Mail Instant Messaging IT Service Management Telephony Telepresence Virtual Teams	[redacted]
Core Services	Compute Hypervisor Network Storage	[redacted]
End User Computing	Peripherals Printers Non-Windows Devices Windows Devices	[redacted]
Management and Support	Alerting and Escalation Backup Infrastructure Management Tools Infrastructure Monitoring Tools	[redacted]

	Log and Event Management Monitoring	[redacted]
IT Security	Application Content Inspection Endpoint Security Identity Management Network Access Control Vulnerability Management	[redacted]

2.2 Out of Scope

The following Technology Infrastructure assets are not in the scope of this document

- **Protection and Control; and**
- **Telecommunications networks (external and wide area networks including SCADA LAN/WAN).**

3 TasNetworks Asset Management

Investment drivers for IT Infrastructure stem primarily from the need to provide services that can maintain the required levels of reliability, efficiency, capacity, and supportability. Increasingly flexibility and agility will be important due to the unprecedented amount of change the business will likely undergo as directed by the TasNetworks Digital Strategy.

Investment is required in order to maintain the currency and supportability of these systems and to cope with both realised and anticipated business growth. Investments in these projects are made to ensure that Corporate IT can continue to provide the required infrastructure to support business requirements and increasingly align with the platforms and processes of other TasNetworks technology departments.

IT equipment has a rapid rate of evolution, with vendors generally superseding products within 3-5 years. This change is partially driven by vendors updating their technology based on the availability of newer components (e.g. chipsets or CPUs), as well as through the implementation of entirely new technologies. The rapid shift in technologies limits the ability of suppliers and vendors to continue to maintain older products, and as a result continued support for older products becomes increasingly expensive or unavailable.

In addition to the evolution in technology, demands on technology capacity are constantly increasing. As a result, older equipment often lacks the capability to deliver services required by the business as business functions evolve.

Finally, the IT industry is experiencing two seismic shifts in the platforms and pricing models relating to delivery of IT platforms:

1. Increasing use of off-premise infrastructure to provide core business infrastructure, platform and software services to internal and external customers (‘Cloud computing’); and
2. Increasing use of subscription pricing models, with a resultant shift of expenditure from CAPEX to OPEX.

Maintaining the IT infrastructure in a state that meets business requirements encompasses the activities and requirements documented in the following subsections.

Lifecycle Replacement

IT Infrastructure and associated software requires evaluation at or (preferably) before the end of its expected life to determine any need for replacement in order to continue supporting business applications. End-of-life equipment no longer enjoys vendor support or maintenance, shifting all maintenance and support costs onto the owner. Additional drivers for lifecycle replacement include:

- Per-year warranty costs increase over the life of the asset;
- Per-instance patching and software upgrade costs increase over the life of the asset;
- The likelihood of software and hardware incompatibilities increases over the life of the asset;
- The number of servers each administrator can manage decreases as the servers become older;
- Baseline operating system performance degrades over time as the servers age; and
- Hardware failure rates escalate during the operating lifetime of the platform;

In addition to the negative consequences listed above to delaying refresh cycles, new assets provide:

- Reduced power and cooling costs;
- Reduced administration costs;

- Greater security and reliability;
- Smaller physical footprint (reduced demand for data centre space); and
- Enablement of modern features and approaches to application delivery.

Capacity Management

The primary objective of Capacity Management activities is to ensure that IT capacity meets current and future business requirements in a cost-effective manner. Capacity Management activities include:

- Forward planning to identify and meet forecast growth and future business requirements;
- Installation, upgrade and replacement of platforms to meet forecast requirements; and
- Ongoing performance monitoring and management of IT systems.

Maintain Software Assurance

TasNetworks IT has a requirement to acquire and maintain software upgrade rights for all infrastructure related software licences and hardware firmware. These rights reduce support costs, allow maintenance of a high level of security and reduce upgrade costs through access to upgraded versions of software.

Software Assurance also guards against software bugs and potential (likely) security vulnerabilities in out-of-date and superseded software versions.

Vendor Technical Support

Appropriate technical support agreements are required to deliver hardware and software support in a manner that meets IT service level requirements. Support requirements include:

- Fault diagnosis and resolution assistance;
- Software patches and updates;
- Firmware and BIOS patches and updates; and
- Hardware break fix support.

For critical systems, this support should be available 24 hours per day, 7 days per week in order to ensure the availability and effectiveness of infrastructure underpinning business application services. Complex systems may require vendor or manufacturer engineers to attend on-site to assist with fault resolution or perform scheduled maintenance activities.

Regulatory Compliance

While some of the items documented in this plan do not have direct current or anticipated regulatory implications, the infrastructure described does support the broader TasNetworks business in the execution of regulatory responsibilities.

Areas with direct regulatory implications have been identified, these are:

- TasNetworks backup and disaster recovery infrastructure supports TasNetworks ability to recover essential business services in the event of a disaster. These services enable the TasNetworks business to meet its regulatory requirements during a declared disaster;
- IT Security infrastructure directly supports TasNetworks efforts to ensure the privacy and protection of critical business assets and data. These efforts enable TasNetworks to meet data privacy and related regulatory compliance requirements;

- IT Security Infrastructure supports key controls to enable compliance with anticipated future cyber security legislative requirements for the energy sector;
- Core infrastructure underpins critical operational and supporting systems, as well as enabling compliance with future critical infrastructure legislative requirements;
- Application delivery infrastructure supports continued application and data availability supporting business service delivery in the event of a lockdown / stay-at-home order; and
- Telephony and contact centre systems provide critical regulated services including; control room operations and providing fault and emergency contact services for the general public.

3.1 Asset Management Influences

While not directly related to the management of IT assets at TasNetworks, the influences discussed briefly below will impact planning, implementation and lifecycle management processes and future strategy and purchasing decisions at TasNetworks.

Technology Trends

Relevant industry trends have been identified during the Determination process; these are discussed in the applicable asset class description sections that follow.

Transformative Technologies

The emergence of transformative technologies (also referred to as disruptive technologies or disruptive innovation) is a regular occurrence in the IT industry due to the rapid rate of technological change and massive ongoing spending in technology research and development. Once implemented and accepted, these technologies may result in significant changes to business processes, operating models and/or market conditions.

Past examples of transformative technologies in the IT industry include:

- The emergence of corporate computing in the 1960s;
- The development and acceptance of the personal computer in the workplace in the 1980s;
- The rapid growth and use if the internet from the late 1990s;
- The use of mobile devices and networks in the last decade;
- The recent rise and popularity of cloud computing and infrastructure; and
- The rise in IoT and convergence of IT and OT technologies.

A number of disruptive technologies can be expected to emerge or gain widespread acceptance over the determination period. Where applicable, both current and potential future disruptive technologies are discussed below.

By their nature, the budgetary impact of transformative technology adoption can be difficult to assess. Therefore in general a conservative approach to determination of both CAPEX and OPEX requirements in the Initiative Assessments within the scope of this plan has been taken.

4 IT Asset Class Description

IT assets include all hardware and software platforms required to deliver application and data access services to the TasNetworks business in a timely and effective manner. The assets listed below serve both 'live' production TasNetworks services as well as:

- Development and testing environments enabling enhancement of existing services as well as new services required by TasNetworks;
- IT Infrastructure services delivered to 42-24 customers on behalf of 42-24; and
- Provision of disaster recovery/service continuity capability to ensure continued access to data and applications.

Investment drivers for IT Assets stem primarily from the need to provide services to meet TasNetworks current and future application and data services requirements. This investment is required in order to maintain currency and supportability of these systems and to cope with user demand, capacity growth and the evolving IT technology environment over the term of this asset management plan.

4.1 Server Hardware

This asset class refers to hardware infrastructure specifically designed for hosting of server applications, primarily (but not necessarily exclusively) in one or more of TasNetworks data centre facilities. Server hardware includes:

- Native Physical Servers: servers running a single operating system instance and one or more applications directly on the physical hardware and without an intervening virtualisation layer;
- Virtualisation Physical Servers: servers running virtualisation software, thereby hosting multiple logical operating instances on the hardware; and
- Server hardware includes the physical servers themselves as well as shared server infrastructure, required for blade server installations (including chassis, power supply and interconnect components).

As at Q1-2022, TasNetworks operates 76 virtualisation server hosts and manages 7 native physical servers.

Servers are typically operated to a 5-7 year life cycle, while shared blade infrastructure components are refreshed less frequently (8-10 years). The nature of the current platform allows staggered generations to co-exist, which allows refresh cycles to be likewise staggered and an optimum 20% refresh per year routinely executed.

4.1.1 Technology Trends

Technology trends shaping server hardware include the following themes:

> *Cloud Infrastructure Services:* No longer a new technology, use of Infrastructure as a Service (IaaS) is increasingly common in the industry, reducing asset requirements and associated CAPEX (with transfer of costs to OPEX). Through 42-24, TasNetworks is a provider of IaaS to other Tasmanian organisations.
>
> While wide adoption of external IaaS services for TasNetworks workloads is not anticipated, cloud providers will be used to host services where such hosting makes sense. Enabling this hosting will require work to integrate on-premises and IaaS workloads and unify management processes.

Near-Ubiquitous Server Virtualisation: server virtualisation can be defined as the partition of a physical server into multiple logical server instances. The benefits of virtualisation include:

1. Increased utilisation of server resources;
2. The ability of servers to survive failure of underlying hardware with minimal disruption to IT service delivery; and
3. Simplified IT backup and disaster recovery.

The overwhelming majority of TasNetworks server workloads are virtualised, and the focus for this technology is to maintain and improve the platform as new hypervisor software versions go to market.

Increasing Capacity: key server components continue to evolve to provide increased processing, memory and storage capacity. The ‘scale out’ of processors to include an increasing number of physical cores in the CPU footprint is both a driver and beneficiary of the trend towards server virtualisation, as is the increase in memory available to each server platform.

Windows Server: a new version of Windows Server (Server 2022) has been released by Microsoft in mid-2021. This release will be supported by Microsoft until the latter half of the decade.

We have recently updated the Windows server standard operating environment (SOE) for new installations to Windows Server 2019. It is expected over the length of the determination period the SOE will be updated at least twice. It is further anticipated that update activities will be resourced from BAU operational support activities and that major application platforms will be updated to the new SOE when major version upgrades take place or other critical drivers come into play.

Linux: the Linux operating system has been widely adopted in the marketplace, with increasing use of the platform to support application delivery (e.g. containers, microservices) and development (e.g. DevOps, CI/CD) architectures.

At this time the Linux OS at TasNetworks fills a critical role, as the SAP Hana database platform is hosted on SuSE. However, in 2020 a review of OS platforms resulted in the selection of Red Hat Enterprise Linux (RHEL) as the preferred Linux OS for future non-SAP applications. This decision was made due to a number of factors, including increased market presence and quality of product support and documentation.

Given the increasing emphasis SAP is placing on deployment of products using SuSE, it remains likely that TasNetworks will continue to manage two Linux environments (being SuSE and RHEL). This is considered manageable given the relatively small footprint and ability to use common management tools in many cases, but will be monitored.

4.1.2 Transformative Technologies

The transformative technologies described below will be regularly evaluated by TasNetworks IT to determine the benefits and risks of implementation. Implementation of the technologies will take place as recommended by review activities:

DevOps: DevOps (a portmanteau of *Development* and *Operations*) aims to bridge the gap between projects and operations by using agile techniques both in development, project management and system administration activities.

Since the last plan update, DevOps (and related practices such as GitOps and DevSecOps) have gained widespread acceptance in the industry (as evidenced by the adoption of DevSecOps by the

U.S. Department of Defence as the preferred technology stack for delivery of reliable and secure applications).

TasNetworks' is actively looking to increase its capability in this area, and has implemented a number of automation tools with the eventual aim of implementing DevOps throughout the core infrastructure landscape. The aims of this implementation include improving security (through deployment of known-secure configurations), reliability (by reducing the risk of incorrect configuration changes) and efficiency (by automating labour intensive deployment and maintenance processes).

Application Containers: A container is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another. A container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings (and can also include telemetry and security capabilities integral to the image).

Container images become containers at runtime. Available for both Linux and Windows-based applications, containerized software will always run the same, regardless of the infrastructure. Containers isolate software from its environment and ensure that it works uniformly despite differences for instance between development and staging.

Requirements to implement, manage and support application containers are anticipated in the lead-up to the next reset period, as software developers and vendors increasingly move towards the platform (for example, Monarch have indicated that their SCADA products will migrate to container platforms in the near to mid-term).

4.2 Storage Hardware

For the purposes of this document, storage hardware refers specifically to infrastructure installed to provide shared storage for servers and server applications as well as general document storage. Storage hardware includes:

- Storage Area Network (SAN) and Network Attached Storage (NAS) infrastructure;
- Fibre Channel switching hardware dedicated to storage access; and
- Presentation of storage directly to consumers via CIFS, NFS and object interfaces.

Both the corporate environment and operational storage environments environment operate on separate pairs of redundant storage arrays. Storage hardware of this type is typically operated on a 4-5 year life cycle as it is considered mid-range. Typically annual maintenance and support charges for such arrays are significantly increased during years 5 and 6 to send a strong price signal to customers to upgrade and replace.

TasNetworks continue to identify and implement measures to control both capital and operational costs of storage infrastructure. Examples include:

- Negotiation of partner status with NetApp (leveraging 42-24's service delivery and product implementer status) to negotiate preferential pricing on both purchase and maintenance of storage platforms, as well as access to extensive platform training and support for the operational team; and
- Working with suppliers and vendors to maximise the effective life-span of storage platforms, potentially deferring major CAPEX purchases.

4.2.1 Technology Trends

Technology trends influencing storage hardware operations include the following themes.

Increasing Demands for Storage: while not specifically a storage technology trend, new application technologies and services are driving an increasing demand for storage capacity. These services include:

- Big Data and massive-scale data warehousing;
- Ubiquitous device connectivity and instrumentation; and
- Increasing use and storage of rich media, including high quality video streams.

The increased volume and diversity of data being stored and new requirements to index, search and analyse this data result in a growing reliance on storage resource management tools to limit the operational overheads accompanying storage growth. This in turn places additional costs on storage acquisition and storage management software licensing.

Increasing Storage Capacity and Density: Fortunately (in light of increasing demands for storage discussed above), storage capacity and density continues to increase. The side effect of these densities are that the controllers becomes the bottleneck after only a single tray of disk, with consequent changes to the controller-storage architecture in modern SAN systems.

Increased Storage Performance: The explosive growth of Solid State Disk (SSD) technologies has enabled a tremendous increase in the performance of data storage platforms. While earlier generations of the technology lacked capacity, reliability or back-end storage bus performance, the technology is now widely deployed across the IT industry.

Relieving or removing performance bottlenecks associated with disk performance does however present new challenges, both in the storage systems themselves (which generally require redesign to take advantage of disk performance) and in overall systems Implementation and management operations (relieving storage bottlenecks often exposes performance constraints in other areas of the system architecture). TasNetworks now operates only SSD technology on primary storage. This has allowed the disk performance to leap ahead of the rest of the stack but does increase pressure on compute and storage controllers.

Storage Network Protocols: while TasNetworks continues to deliver storage to consumers over the Fibre Channel protocol, industry focus is shifting to protocols that operate over Ethernet networks (such as FC over IP and FC over Ethernet as well as iSCSI). This focus is largely driven by the increase in Ethernet technology performance to meet and surpass that economically available over Fibre Channel.

While TasNetworks will continue to operate Fibre Channel storage networks in the immediate future, subsequent platform replacement cycles will review the performance and cost efficiency of Ethernet-based storage networks against the status-quo, and upgrade or replace as appropriate.

4.2.2 Transformative Technologies

‘Big Data’: Big Data is a broad term for data sets so large or complex that traditional data processing applications are inadequate. Challenges include analysis, capture, search, sharing,

storage, transfer, visualisation, and information privacy. The term can also refer to the use of predictive analytics or other advanced methods to extract value from data.

Analysis of data sets can find new correlations unavailable to traditional data processing methods. IT departments across most industry sectors are encountering large data sets in areas including Internet search, finance and business informatics.

Data sets grow in size in part because they are increasingly being gathered by cheap and numerous information-sensing mobile devices, aerial (remote sensing), software logs, cameras, microphones, radio-frequency identification (RFID) readers, and wireless sensor networks. Relational database management systems and desktop statistics and visualisation packages often have difficulty processing these data sets. The work instead requires "massively parallel" software running on tens, hundreds, or even thousands of servers.

Given the nature of TasNetworks business, including the potential future use of sensor and drone technologies to monitor the state of the transmission and distribution, this technology is likely to have an impact on data processing and storage operations. Adoption of the technology will require new approaches to systems design and the adoption of platforms and products to match.

Convergence and Hyper-Convergence: TasNetworks has no plans as this stage to implement converged or hyper-converged storage/compute architectures. However, developments in the area will continue to be monitored.

4.3 Network Infrastructure

Location	Hardware Type	Description/Notes	Typical Lifespan
TasNetworks Data Centres	Core Switch	A high-capacity switch generally positioned within the backbone or physical core of a network. Core switches serve as the final aggregation point for the network. Core switches in use at TasNetworks include: • Cisco Nexus 9300/9500	7-10 years
	Server Switch Fabric Extender	Hardware connecting data centre servers to the core switch. Note that many devices (including server chassis interconnects) will connect directly to the core switch infrastructure. A fabric extender is a specialised piece of hardware that physically 'extends' a data centre switch by providing port capacity in a discrete form factor that is physically detached from the parent switch. Examples of these hardware types in use include: • Cisco Nexus 9300 • Cisco Nexus 2000 • Cisco Catalyst 9500 • Palo Alto Firewalls	6-8 years
	Router	A device used to forward data between networks. Typically used to provide access to external networks or remote sites. In-use example:	6-8 years

		• Cisco 4000 ISR Routing functions may also be performed by appropriately specified and configured switch hardware.	
Site Locations	Access Switch	Provides physical connectivity to endpoint devices, including workstations, printers and telephony equipment. Models in use include: • Cisco Catalyst 3850 • Cisco Catalyst 4500 • Cisco Catalyst 9300	6-8 years
	Wireless Access Point	Allows wireless devices to connect to the wired network. TasNetworks currently used the following access point models: • Cisco Catalyst 9120 • Cisco AiroNet 3x00	3-5 years
	Wireless LAN Controller	Used to manage multiple wireless access points and regulate wireless access to the network. TasNetworks currently uses the following WLC models: • Cisco Catalyst 9300 • Cisco AiroNet 5508	5 years
	Router	Used in remote sites to access communications links to TasNetworks data centres. Examples include: • Cisco V Edge 1000 • Cisco V Edge 100M • Cisco V Edge Cloud • Cisco CAT 8500	6-8 years

The Infrastructure team is responsible for the operation and periodic replacement of more than 810 such devices across Tasmania.

4.3.1 Technology Trends

The network technology trends discussed below have been considered when planning the program of work for the determination period.

Increased Remote Working: The trend towards increasing uptake of home, remote and mobile working at TasNetworks was sharply accelerated by the COVID pandemic (ongoing as of this document update). During the height of pandemic lockdown restrictions, TasNetworks was able to successfully transition the vast majority of its non-field workforce to home work. This success (at short notice) was largely due to existing investments in technology platforms enabling secure remote working.

Acknowledging that remote and home work is now part of normal business operations, IT will continue to invest in enabling technologies, aiming to extend the reach, improve user experience and the security of remote access infrastructure.

Network Security: In the light of the increasing frequency and impact of cyber security events, the security and integrity of networks has become critical to the continued business operations. Efforts to improve TasNetworks security posture and capabilities are particularly relevant to data network operations, as the network is the vector for both compromise of systems and exfiltration of data.

Architectures and tools to improve network security include *zero trust networking* – where data traversing between nodes on the network is assumed to be unauthorised unless explicitly vetted and allowed and use of *artificial intelligence* and *machine learning* to prevent, detect and respond to network intrusion attempts.

TasNetworks will continue to evaluate and implement technologies and processes to improve network security and reduce associated risk.

Increased Data Centre Network Bandwidth: TasNetworks core network interconnects currently utilise 40 and 100-gigabit Ethernet transmission protocols over fibre optic media. This capability was introduced with the implementation of Cisco Application Centric Infrastructure (ACI) hardware and software at the Cambridge and Derwent Park datacentres.

Network Protocol Convergence: TasNetworks currently maintains separate network infrastructure for storage (Fibre Channel) and general network traffic (Ethernet). As the available bandwidth of both types of networks increases, many organisations are choosing to consolidate network architectures into a single type of network (although storage and general networks usually remain physically separated), using one or more converged network protocols (which allow the encapsulation of one communications protocol inside of another to facilitate the transmission of both types of data).

As part of infrastructure refresh activities for both storage and data centre LAN infrastructure, the use of converged network infrastructure throughout the communications path will continue to be evaluated, but no action is envisaged during the current reset period.

4.3.2 Transformative Technologies

Cloud Computing: Discussed above, the widespread deployment of Software, Platform and Infrastructure-as-a-Service computing will place an increasing reliance on the availability and performance of WAN interconnects and internet connectivity.

Internet of Things: Or IoT - describes physical objects (or groups of such objects), that are embedded with sensors, processing ability, software, and other technologies, and that connect and exchange data with other devices and systems over the Internet or other communications networks. Use of IoT technology and platforms requires particular care to be taken to ensure the stability, performance and security of the connective network.

There are a number of concerns about the risks in the growth of IoT technologies and products, especially in the areas of privacy and security, and consequently, industry and governmental moves to address these concerns have begun, including the development of international and local standards, guidelines, and regulatory frameworks.

TasNetworks currently operate IoT networks in the (power) network operations space, this use will almost certainly expand in scope and functionality over the remainder of this reset period and through the next.

Software Defined Networking: Software Defined Networking (SDN) is an approach to computer networking that allows network administrators to manage network services through abstraction of functionality. This is done by decoupling the system that makes decisions about where traffic is sent (the control plane) from the underlying systems that forward traffic to the selected destination (the data plane).[1]

Advantages of SDN include:

- Directly programmable: Network control is directly programmable because it is decoupled from forwarding functions;
- Agile: Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs;
- Centrally managed: Network intelligence is (logically) centralised in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch;
- Programmatically configured: SDN lets network managers configure, manage, secure and optimize network resources very quickly via dynamic, automated SDN programs. The programs are easily written because they do not depend on proprietary software; and
- Open standards based and vendor neutral: When implemented through open standards, SDN simplifies network design and operation because instructions are provided by SDN controllers instead of multiple, vendor-specific devices and protocols.

Cisco has introduced SDN into their product offerings through the Nexus 9000 series of data centre switch platforms. These platforms have been implemented successfully at TasNetworks.

SD-WAN (software defined wide area network) has also been implemented at TasNetworks. will be evaluated in the short to medium term. This offers the ability to use multiple carriers and link technologies to aggregate and prioritise traffic from remote sites based on policy.

SD-Access (software defined access layer) technologies and products may be implemented at TasNetworks prior to the end of the current reset period, subject to analysis of benefits and availability of implantation resources.

Optimisation of the above technologies will continue into the R24 reset period.

4.4 Client Hardware

Client hardware includes all endpoint devices connecting to the TasNetworks network infrastructure and accessing TasNetworks data and/or applications. This hardware includes:

- Desktop computers
- Laptops and notebooks
- Mobile phones
- Tablets

The recognition of the importance of mobile phones for clients to access corporate systems has meant a formal adoption of a lifecycle and strategy for these non-windows devices. The definition also includes network-connected printers and multifunction devices.

[1] http://en.wikipedia.org/wiki/Software-defined_networking

The table below lists the types and number of client devices supported by TasNetworks IT as of January 2023, including supporting peripherals.

Type	Quantity	Typical Lifespan
Desktop Computers	~200	3 – 5 years
Laptop/Notebook Computers/Convertibles	~1450	3 – 5 years
Mobile Phones	~1100	3 - 5 years
Supporting peripherals (monitors, docking stations)	~2000	3 – 6 years

4.4.1 Technology Trends

Remote Working: The COVID-19 pandemic has sharply accelerated the trend towards increasing home and remote working at TasNetworks, and while Tasmania was fortunate enough to be spared the worst of the outbreak, for several months during 2020 the majority of the workforce (and nearly all office workers) worked from home. The technologies and platforms stood up or extended to accommodate lockdown have been operationalised to accommodate home and work remote options as an employee preference as well as to allow business operations to continue unimpeded if further lockdowns become necessary.

Support for home working has had a flow-on effect of improving TasNetworks ability to support the field workforce through improved network access. Efforts are also ongoing to strengthen the security of the remote access service as part of the Cyber Security program of work.

Windows 10 Release Cadence: Windows 10 is the standard operating system for desktops and notebooks at TasNetworks, and is installed on all devices (outside of a small number of specialised devices that cannot yet be upgraded).

The semi-annual release cadence of Windows 10 has required TasNetworks to be effectively continually upgrading the desktop/notebook fleet to ensure that desktops remain supported. It is hoped that the switch to annual releases with the release of Windows 11 (see below) will reduce the overheads associated with maintaining the desktop fleet.

Windows 11: Windows 11 was initially released to new devices only. Although Microsoft has committed to providing support for Windows 10 (assuming that release updates are applied) to mid-2025, however before that date it is almost certain that TasNetworks will no longer be able to purchase new devices with Windows 10. Therefore, evaluation of the platform will take place before introducing the operating system in order to ensure that any future installations can be fully supported in the TasNetworks operating environment.

Microsoft 365: TasNetworks has purchased Microsoft 365 licensing for all users, and is currently in the process of rolling out product functionality (see Collaboration below). As part of the rollout, desktop office applications will be migrated from Office 2016 to Office 365. From that point, the desktop productivity suite will be subject to Microsoft's continuous product release cadence, this will require additional management by the IT infrastructure and desktop support teams.

Cloud Management: Management tools for endpoint devices are increasingly moving from on-premises installations to cloud SaaS offerings. This trend presents a few challenges, including:

- Ensuring the security of cloud management platforms; and
- Funding future software purchases as operational expenditure.

TasNetworks will continue its current reactive stance to this trend, seeking to capitalise software purchases when possible and appropriate, but retaining the ability to migrate to cloud subscription solutions where necessary.

4.4.2 Transformative Technologies

Cloud Desktops: Microsoft has recently released its cloud-based desktop service, Windows 365. This service allows users to connect to a persistent desktop hosted in Microsoft datacentres from any authorised device. Aimed primarily (at least initially) at corporate users, desktops can be integrated with on-premises application and identity management infrastructure through Microsoft Azure and Azure Active Directory.

Will there is no pressing need to adopt this technology, evaluation will take place to prepare the product for introduction in the event that a compelling use-case is identified.

4.5 Security Hardware and Software

During the current reset period, global cyber security events have driven an increasing focus on TasNetworks ability to effectively secure hardware and software assets, detect and respond to cyber security incidents and contain or mitigate successful intrusions. While much of the security uplift activity has been (and continues to be) carried out by the Cyber Security Program and team, IT Infrastructure remains responsible for many operational aspects of IT security, including the management and operation of tools supporting cyber security controls.

Investment drivers for security systems stem primarily from the need to provide services that be delivered reliably, effectively and securely. The investment is needed to maintain currency and supportability of these systems and to cope with user demand, meet performance requirements as well as responding to the evolving security environment. IT security platforms and processes are (and will continue to be) integral to management of all IT Infrastructure assets over the term of the asset management plan.

The high-level strategic objectives of IT security systems are to:

- Ensure the integrity and confidentiality of TasNetworks data;
- Protect TasNetworks IT infrastructure against targeted attacks;
- Block unwanted, offensive and malicious content from entering the corporate network;
- Provide secure and reliable remote access over un-trusted public networks;
- Detect and respond to security incidents in order to correct damage and evaluate incidents that have occurred; and
- Effectively respond to security incidents.

The scope of installed security platforms includes:

Perimeter security platforms, such as -

- Intrusion Detection (IDS) and Intrusion Prevention (IPS) Systems;
- ‘Edge’ network firewalls;
- Internet mail and web access filters; and
- Remote access gateways and associated infrastructure;

Network security platforms, including Cisco Identity Services Engine (ISE) and internal network firewalls;

Endpoint security software (antivirus/antimalware and endpoint firewall software);

Network monitoring and log analysis tools; and

Identity management and authentication, authorisation and accounting systems.

4.5.1 Technology Trends

Evolving Threat Landscape: Threats to IT systems and data are rapidly evolving in complexity and capability. In addition to the increasing sophistication of attacks by criminal organisations, unfriendly nation-states and non-state actors (both terrorist and activist organisations), many of the technology trends described elsewhere in this document enable new vectors for compromise of IT systems and data. Examples include:

- Increasing use of mobile devices in the enterprise;
- Adoption of cloud computing; and
- Interconnected devices.

Recent developments include the compromise of hardware and software supply chains and the exponential growth in ransomware attacks on business and government entities.

In order to avoid or mitigate the technical, financial and reputational impact of security breaches, TasNetworks will continue to implement, upgrade and maintain security platforms as outlined in the IT Security Investment Evaluation Summary. Additionally, the need to maintain the security and integrity of IT systems is a driver for many of the infrastructure upgrade and replacement activities documented in other Investment Evaluation Summaries.

4.6 Microsoft Software and Platforms

Microsoft server and client software is extensively used at TasNetworks and constitutes the greater part of software licenses by both cost and number installed. The software is critical to the delivery of application and data services in support of TasNetworks Transmission and Distribution businesses.

Microsoft software in use at TasNetworks includes:

- Microsoft Windows operating systems (both server and desktop);
- Desktop productivity applications delivered by Microsoft Office;
- Server and ‘back-office’ applications, such as Microsoft Exchange Server and SharePoint; and
- IT Service Management applications contained in the System Centre suite.

Most Microsoft software is licensed by TasNetworks under the terms of their Enterprise Agreement (EA) with Microsoft Australia (server and some desktop software), or TasNetworks Microsoft 365 subscription (desktop productivity and collaboration tools plus supporting infrastructure hosted and operated by Microsoft).

The Enterprise Agreement is renewed every three years, with annual updates to license counts on the anniversary of the agreement, whereas the Microsoft 365 subscription is renewed annually.

4.6.1 Technology Trends

Technology trends regarding server and client software are discussed in the respective preceding sections of this document.

4.6.2 Transformative Technologies

Software as a Service: Microsoft is increasingly offering software applications under a subscription model and are aggressively encouraging migration to these services. These offerings include:

- Microsoft 365: Formerly Office 365, Microsoft 365 is the brand name used by Microsoft for a group of software-plus-services subscriptions that provides productivity software and related services to subscribers. For business and enterprise users, Office 365 offers plans including e-mail and social networking services through hosted versions of Exchange Server, Lync, SharePoint and Office Web Apps, integration with Yammer, as well as access to the Office software.
- TasNetworks has taken up the use of Microsoft 365, initially with the introduction of Microsoft Teams to support collaboration activities and replace Microsoft Skype for Business. Use of other parts of the Microsoft 365 service stack will be adopted in a judicious manner to maximise the return on investment in the subscription.
- Microsoft Azure: Microsoft Azure is a cloud computing platform and infrastructure, created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed data centres. It provides both PaaS and IaaS services and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems.

Considerations and implications for hosting TasNetworks application and data services on this platform are discussed in Server Hardware.

4.7 Other Server and Client Software

This category embraces all non-Microsoft software licensed by TasNetworks for both client and server platforms. Most such software falls outside the scope of this document, but a number of platforms are managed by IT Infrastructure, including (but not limited to):

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.7.1 Technology Trends

Software as a Service (SaaS): many vendors are now offering software services as a service offering hosted externally to the customer (either on vendor infrastructure or increasingly over major infrastructure service providers). This architecture has matured to the point where it is the preferred service delivery model for many software vendors.

Use of SaaS offerings offers particular attractions for services where specialised support skills are difficult and/or expensive to acquire and maintain, or are considered outside the scope of services that reasonably can be provisioned and supported by in-house IT departments. In these cases, use of SaaS offerings can allow deployment of these application services under circumstances where they would otherwise be not practical.

As with all cloud computing services, care and attention needs to be paid to maintaining the security, longevity and service levels of these services holding TasNetworks data. Increasingly vendors are moving towards 'owning' derived data in a system and extracting business data from these systems for other uses without appropriate licenses has led to several public large monetary impacts. This comes as vendors and increasingly aware that 'data is the new currency.' An additional complication to be addressed is the impact of these services on operational budgets where previously it was preferable to favour development capital assets.

4.7.2 Transformative Technologies

Infrastructure As Code: closely related to DevOps and DevSecOps models discussed above, is the process of managing and provisioning computer data centres through machine-readable definition files, rather than physical hardware configuration or interactive configuration tools. The IT infrastructure managed by this process comprises both physical equipment, such as bare-metal servers, as well as virtual machines, and associated configuration resources. The definitions may be in a version control system.

Telemetry and On-Premises Data Analytics: Applications, operating systems, networks, security software, client devices, the Internet of Things (IoT), and other technologies generate a significant amount of event and machine data. Monitoring and analysing machine data can solve many problems. However, machine data is complex, and enterprises face significant challenges in converting it into timely and actionable information.

Telemetry processing and analytics engines harness big data and AI to enable identification and analysis of trends and timely reaction, but is highly resource-intensive, particularly for compute resources.

Hosted and Service-Based Data Analytics: also known as Big Data as a Service (BDaS), these services leverage the massive amounts of compute and storage capacity available in public IT service provider infrastructure to provide large scale data analysis services with little or no need for expensive on-premises infrastructure. These services can often integrate other public and private data services into the analytics process (for example geospatial and social networking data) that would not otherwise be available.

These services are particularly useful for processing large data sets where the data processed is of low business sensitivity, but as always caution is advised for more sensitive data, including referencing data privacy, integrity and sovereignty requirements before adoption. Consideration for the increasing demand for internet bandwidth and availability should also be factored.

5 Asset Maintenance & Lifecycle

The TasNetworks IT Infrastructure Team is responsible for the management, implementation and support of all the system assets discussed in this Asset Management Plan. A summary of general lifecycle reviews/dates is shown in the following table.

Asset	Event	Timeframe	Driver
Server	Server replacement	Annual on a rolling basis, server lifespan 5-7 years	To adequately support business and operational IT systems through the provision of reliable and fit for purpose IT infrastructure. Replace equipment within a suitable economic lifespan, maintaining active vendor warranty support to facilitate timely remediation of any hardware faults.
Storage	Storage array replacement.	2022, 2027	As above
Network	Data centre network equipment replacement	2021, 2026 (Core switch hardware) Rolling upgrades to replace end of support equipment.	End of life is determined by the cessation of product support and security updates.
Network	Office location network equipment replacement	Semi-annual Rolling upgrades as equipment reaches end of life	End of life is determined by the cessation of product support and security updates.
Network	Wireless network equipment replacement	Generational upgrades 2021, 2026. Semi-annual Rolling upgrades as equipment reaches end of life	End of life is determined by the cessation of product support and security updates.
Client Hardware	Desktop/laptop replacement	4 – 5 year anticipated lifespan for individual devices, subject to continued hardware and software support.	
Client Computing	SOE refresh	Semi-annually going forward as Microsoft has changed cadence with Windows 10.	Maintain current supported OS and core applications. Upgrade cadence will be reviewed in 2022 to match the Windows 11 release cadence.
Microsoft Software	Enterprise Agreement	3-yearly renewal, annual true-up. Office upgrades scheduled for 2022 (to Office 365),	

		then as required by the Office release cadence.	
Microsoft Software	System Centre version upgrades	Semi-annual upgrades to Configuration Manager and Operations Manager as released by Microsoft. Service Manager is planned to be retired in 2022.	Maintain current supported application versions
Microsoft Software	Exchange version upgrades	Migrate to Exchange Online before October 2025	Dependency on EDRMS. Upgrades delivered by Microsoft following migration.
Microsoft Software	Teams	Client upgrades as pushed by Microsoft. Server components maintained and upgraded by Microsoft.	
Other Software	NetMotion Suite	2021	
Security Software	Web filter, mail filter upgrade or replacement	Web filter TBD Mail filter 2022	Web filter upgrade plans may change depending on Data Loss Prevention software selection and implementation.
Security Software	Network Access Control system upgrade or replacement	2022, 2026	As above
Security Software	Endpoint Security (Client and Server)	2025	Upgraded in 2020/21, future upgrades subject to evaluation of product options.
Security Software	Application control software	TBD, 2022+	Subject to evaluation of options in 2022.
Security Software	SIEM and Remote Access system upgrade or replacement	2025	Major upgrade completed in 2021.
Security Hardware	Firewall replacement	2025	Replace equipment within a suitable economic lifespan, subject to support availability. Maintain up to date security controls to keep up with evolving threat landscape.

5.1 Condition Monitoring Practices

TasNetworks has adopted a strategy of implementing both proactive and reactive condition monitoring of IT assets, including physical, virtual and software assets.

The goal of proactive monitoring is to predict likely incidents with sufficient notice and actionable alert information to enable IT staff to take corrective action and avoid any system outages.

Reactive monitoring aims to detect incidents affecting IT assets as quickly as possible during or after they occur, to capture sufficient information for the incident to be rectified as quickly as possible.

TasNetworks operates several systems to monitor the infrastructure discussed. These systems are continually undergoing configuration updates to ensure functionality and fitness for purpose. Primary monitoring platforms in use are:

- Microsoft System Center;

- OpVizor;
- Splunk;
- Cisco DNA Center; and
- Palo Alto Panorama.

5.2 Defect Management

Infrastructure defects are managed through the Service Request, Incident and Problem Management processes and implemented within the IT Service Management tool. A key component of this system and these processes is the front line Service Desk, who field telephone calls and email requests. The Service Desk escalates calls to the Infrastructure Team, as well as incidents or tickets being raised by the alerting and monitoring systems directly.

The current tool is ageing, and presents significant usability and supportability issues. While long term replacement will be aligned with T&P efforts to standardise toolsets across business units, in the short to medium term IT are investigating Jira Service Management as an ITSM platform to replace Service Manager.

6 IT Infrastructure Asset Issues

6.1 Server Operating System Age and Support Availability

The most widespread issue facing the infrastructure assets in the scope of this plan is the age of operating systems running on servers. This is a difficult challenge to address as it relies on the systems and software being compatible with current operating systems.

While deploying a new set of servers with a current operating system is relatively straightforward, it is often a difficult and complex undertaking to upgrade or redeploy the software application itself, particularly if the application has been modified, customised or is no longer maintained by the vendor.

Continuing to host servers where the operating system is no longer receiving vendor security updates creates a cyber security risk to TasNetworks that requires ongoing management and mitigation, adding to the operational overhead of managing that host.

At the time of writing, the current support state of various operating systems is as follows:

- 282 (25%) servers are in Extended Support (end of Mainstream Support); and
- 7 (0.6%) servers are Out Of Support.

6.2 Complexity and Overheads

The IT Infrastructure asset environment is becoming steadily more complex due to:

- The increasing number of managed platforms;
- The Increasing diversity of managed platforms;
- Increasing network complexity – including growth in network segments and the need to manage external and cloud networks;
- Support for more application workloads; and
- Requirements to support mobile and remote working.

As a result, traditional methods and tools for managing IT infrastructure hardware and software platforms are becoming less capable of allowing timely management, upgrade and issue/fault resolution. In parallel, the amount of time required to securely operate and manage these platforms has grown.

In response to this trend, IT Infrastructure continues to examine and (where appropriate) adopt tools and processes to automate infrastructure platform operations.

6.3 IT Security Requirements / Evolving Threat Landscape

The sophistication, capability and frequency of cyber security threats and threat actors continues to grow, and has led to many high profile incidents globally. As a critical infrastructure service provider, TasNetworks must ensure that critical systems and data can be protected against unauthorised access, dissemination of confidential information and disruption to service delivery.

The federal government (through the market regulator) is in the process of mandating compliance with strict cyber security standards for the energy and utilities sectors, and TasNetworks customers also expect that our systems are protected from cyber security threats. While work to improve the effectiveness of cyber security controls is led by a dedicated program within TasNetworks, IT Infrastructure plays (and will continue to play) a critical role in implementing, operating and maintaining these controls.

7 Initiatives

The following initiatives were categorised using Technology/Service Reference Models as a guide. Each initiative may represent several distinct projects across the determination period. These projects have been costed and grouped into the following initiatives.

7.1 Infrastructure Core Services

Items that provide the three pillars of IT infrastructure, Network, Compute and Storage across the enterprise. This includes OT environments.

At a high level the initiative scope extends to:

- Maintenance, upgrade, extension and replacement of storage arrays, compute stacks and core network hardware;
- Maintenance, upgrade, extension and replacement of supporting software and management components dedicated to these core components including the hypervisor;
- Maintenance, upgrade, extension and replacement of supporting hardware dedicated to the storage arrays (storage fabric); and
- Implementation of platform functionality to support TasNetworks strategic initiatives.

Initiative	Summary	Estimated / Required Delivery
R19 R24	Infrastructure Core Services	• Hardware refresh as indicated above on a rolling annual schedule. • Capacity upgrades as required, no greater than annually.

7.2 Collaboration Services

Technology that enables collaboration and virtual presence for employees. These include email, chat and video mediums. Email is arguably the heaviest used digital communication form within most enterprises and as such is considered essential to all modern businesses. This includes all management components of these services.

At a high level the initiative scope extends to maintenance and upgrades to:

- Mail and scheduling platforms;
- Team collaboration and conferencing;
- ITSM tools; and
- Telephony platforms and contact centre applications.

Additionally, planned activities include work to expand the functionality of in-use collaboration platforms as well as replacement of platforms as required to ensure continued vendor support.

Initiative	Summary	Estimated / Required Delivery
R19 R24	Collaboration Services	• Software refresh as required to maintain vendor support for the product.

		- Hardware refresh as indicated above on a rolling annual schedule. - Architecture changes as required to support IT strategic goals.

7.3 End User Computing

Items that provide the end user with access to systems. This takes the form of desktops, laptops, tablets, mobile phones and associated accessories (in the future AR and VR components will fall into this category). Please note that a large proportion of software licensing is documented in Platform Software or elsewhere within the determination streams.

End User computing activities within this initiative will maintain the functionality, supportability and security of end user devices used at TasNetworks to access business applications and data.

Initiative	Summary	Estimated / Required Delivery
R19 R24	End User device Fleet	- Hardware refresh as indicated above on a rolling annual schedule. - Additional replacement as required to maintain vendor hardware and operating system support. - SOE changes to maintain operating system support and support new devices. - Software upgrades as required to maintain vendor support.

Table 1 – End User Computing Initiative Summaries

7.4 IT Infrastructure Support and Management Tools

Technology that enables supporting services and management of IT and OT platforms. It covers a wide range of hardware and software platforms required to deploy, configure and monitor infrastructure as well as alerting and event management/ analytics tools.

Activities in this initiative will maintain and improve IT support and management capabilities through:

- **Replacement of management platforms supporting IT operations to ensure continued functionality and support;**
- **Lifecycle replacement of infrastructure enabling backup and archive platforms;**
- **Adoption of server lifecycle and automation components to reduce operational overheads associated with infrastructure management;**
- **Maintenance, upgrade, extension and replacement of system monitoring services ; and**
- **Maintenance, upgrade, extension and replacement of central logging, telemetry and infrastructure analytics services.**

Initiative ID	Summary	Estimated / Required Delivery

R19 R24	IT Infrastructure management platforms	• Hardware and software upgrades/replacement as required to maintain vendor support. • Extension of existing toolsets to provide additional functionality.

7.5 Application Delivery

Application Delivery hardware and software enables delivery of application services and data to end users.

At a high level the initiative scope extends to:

- Infrastructure underpinning application deployment, access and management;
- Remote access infrastructure (excluding security and authentication platforms);
- Application and desktop virtualisation technology options; and
- Application packaging and deployment tools.

Initiative ID	Summary	Estimated / Required Delivery
R19 R24	Application Delivery platforms	• Hardware components replaced as above, on a rolling annual basis. • Software components upgraded or replaced as required to maintain vendor support. • Extension or replacement of platforms to provide additional functionality in support of strategic goals.

7.6 IT Security

Items that cover systems positioned within both the OT and IT environment responsible for inspecting, auditing and restricting system interactions (security systems).

Additionally these services are responsible for extending the security past the network layers to include application and operating system levels. They are responsible for sanitising the data payload and enforcing role based access controls and auditing on many layers.

At a high level the document scope extends to hardware and software dedicated to insuring provision and maintenance of controls addressing cyber security risks. These controls include:

- Network firewalls and intrusion prevention systems;
- Identity and Access Management platforms;
- Endpoint security and associated management tools;
- Internal and external audit of cyber risk controls; and
- Implementation of new controls as mandated by and in conjunction with the Cyber Security Team.

Initiative ID	Summary	Estimated / Required Delivery
R19 R24	IT Security hardware and software platforms	• Upgrade or replacement of platforms to ensure continued functionality and vendor support.

		• Configuration of platforms to provide new or improve existing controls. • Periodic review and possible replacement of platforms to ensure continued fitness for purpose in the evolving cyber security environment.

8 Program of Work

8.1 Project Definition and Selection

The initiatives have been prioritised on the basis of several key factors:

- Level of dependence of other systems (e.g. quality of shared storage has a large impact on many other aspects of IT systems);
- Level of flexibility with regard to scope or cost (e.g. software licensing costs are essentially unavoidable, unless systems are decommissioned altogether); and
- Variability of scope (some initiatives have elements of their scope which could conceivably be reduced, whereas other initiatives are effectively all or nothing).

8.2 Priority List

Priority	Initiative	Est/Req Delivery	IES Option 1 5yr TOTEX	IES Option 2 5yr TOTEX
Must have	IT Infrastructure – Core Services	Annual	$16.2M	$19.4M(+20%)
Must have	IT Infrastructure – Security	Annual	$2.9M	$3.5M (+20%)
Must have	IT Infrastructure – Management and Support	Annual	$4.3M	$5.2M (+20%)
Must have	IT Infrastructure – Collaboration	Annual	$11.1M	$12.2M (+10%)
Must have	IT Infrastructure – Application Delivery	Annual	$1.1M	$1.4M (+20%)
Must have	IT Infrastructure – End User Computing	Annual	$6.0M	$6.3M (+5%)