



# ICT STRATEGIC PLAN

2023-2026 Refresh  
Resolution: OCM 024-24/25

 @ShireofQuairading

 @QuairadingCaravanPark

 @shireofquairading



**CONTENTS**

Section One: Executive Summary ..... 3

Section TWO: Future Goals & Strategy ..... 4

Section Four: ICT Trends for Organisations ..... 6

Section Five: Strategic Plan ..... 9

1 Backups & Disaster Recovery ..... 9

2 Domain ..... 12

3 Antivirus ..... 14

4 Corporate Applications ..... 16

5 IT Support Arrangements ..... 19

6 IT Disaster Recovery Plan ..... 21

7 Internet Gateway ..... 23

8 ISP Links ..... 25

9 Uninterruptable Power Supply ..... 27

10 Computer Room ..... 29

11 Local Area Network ..... 31

12 Desktops / Laptops ..... 33

13 Servers ..... 35

14 Storage ..... 36

15 IP Telephony ..... 37

16 Printing ..... 38

Appendix A: Workstations / Tablets / Laptops ..... 55

Appendix B: Printers ..... 57

Appendix C: Microsoft Licenses ..... 58

Appendix D: Additional Licenses – SynergySoft and Altus ..... 59

Appendix E: Summary of Estimates ..... 60

Glossary of Terms ..... 61

## SECTION ONE: EXECUTIVE SUMMARY

The Shire of Quairading recognizes the evolving landscapes of both its internal and external environments. Embracing technology is crucial for enhancing its services, necessitating a unified approach to the adoption, application, and maintenance of technological tools, in harmony with the Shire's resources and objectives.

The ICT Strategic Plan outlines the Shire's vision for addressing immediate and future technological needs. It underscores the importance of leveraging advanced technology to prioritize both in-house and external customer services. This plan serves as a blueprint for adeptly managing IT, with its core aim to bolster the Shire's mission and amplify the efficiency of services to its community and stakeholders.

Future technological endeavours will span several departments, all converging towards a singular mission: to serve its community, the general public, and other interested parties. In this context, technology emerges as a pivotal tool for communication, integration, data exchange, and resource allocation. Additionally, it paves the way for cost savings by enhancing service efficiency through a unified technological architecture and standards.

This strategic document encourages inter-departmental synergies and promotes collaboration, rather than restricting individual departmental initiatives. It draws upon a balanced IT management approach, combining the strengths of both centralized IT governance and external IT support. A key component of the plan is the formulation of IT architecture and standards, essential for achieving scalability and seamless integration.

The IT Plan of the Shire of Quairading emphasizes a customer-centric approach to technology management. Internally, it champions teamwork, collective decision-making, and equipping staff with the right tools. Externally, it is committed to delivering anticipated services to its community, the public, and other stakeholders.

This Strategic Plan is dynamic, adaptable to the ever-changing technological landscape and the Shire's evolving needs. Serving as a guiding beacon, it ensures that the Shire's technological pursuits align with its overarching objectives, facilitating enhanced service delivery. All technological choices should be strategically driven, as outlined in this plan, guaranteeing decisions are flexible yet aligned with the Shire's aspirations.

**SECTION TWO: FUTURE GOALS & STRATEGY**

This ICT Strategic Plan Update will cover the period between July 2023 and June 2026. Some key goals include the following;

Project	Goal	ICT Trend
Altus	Implement new modules to provide mechanisms to automate repetitive tasks whilst integrating with existing SynergySoft GL.	Intelligent Apps and Analytics
Collaboration Tool	Adopt a collaboration tool that includes chat, video and sharing of content between internal staff. Functionality can include the ability to invite external contacts.	Multichannel Citizen Engagement
Computer Replacement Program	Define a structured program to replace office computers with standardised equipment based on a lifecycle. Adopt a standard operating environment (SOE) to help reduce IT support costs.	Digital Workplace
Cyber Awareness Training	Subscribe to an awareness training program for all employees. Such a platform should continually test employees based on a frequency and not be a once-off test.	Continuous Adaptive Risk and Trust
Data Backups	Instigate a new regime to meet backup retention needs and archival requirements. At any point in time three copies of the corporate data should exist being the live copy onsite, a backup copy onsite and a backup copy offsite.	Cloud to the Edge
Firewall Upgrade	Introduce deep packet inspection (DPI) firewalling so that incoming and outgoing traffic can be scanned for malicious content. Firewall capability should support two or more Internet links.	Continuous Adaptive Risk and Trust
Internet Communications	Implement a business grade, non-contended Internet link as a primary service. Implement a residential grade Internet link as a secondary service. Both links are to support utilising future cloud based applications.	Cloud to the Edge
Intranet Design	Implement an Intranet for the ability to share and manage content. An application can empower teamwork and help to quickly find information that seamlessly collaborates across the organisation.	Intelligent Apps and Analytics
IP Telephony	Upgrade the copper voice phone system. A virtualised phone system can deliver softphone capabilities for iOS, Android and Windows. A secure feature called SIP (calls over the Internet) can be used to reduce calls costs.	Digital Workplace
IT Policy Review	Ensure a document that defines roles and responsibilities, password requirements, granting/revoking access, account reviews and asset management/disposal.	Continuous Adaptive Risk and Trust
Multi Factor Authentication	Tighten security relating to Office 365 and WFH. Two Factor Authentication (2FA) to be implemented into the existing IT landscape for any IT related activities completed outside the office.	Digital Workplace

<b>Project</b>	<b>Goal</b>	<b>ICT Trend</b>
Microsoft Defender for Endpoint	Implementation of Microsoft Defender for Endpoint AV/EDR protection software to provide best-in-class security for endpoints across the organisation.	Security
Patching	Implement a new program that uses a test group for Windows computers prior to all computers receiving an update. Manage the installation of third party apps such as Adobe, Java etc. to address security concerns.	Continuous Adaptive Risk and Trust
Security Solution	Implementation of a specific ICT Security Solution with the implementation of the ACSC Essential 8 Framework.	Security
Work From Home	Build the Work From Home (WFH) strategy into the business. Easy to use technologies will aid in securely working from outside the office. A WFH policy is required.	Digital Workplace
Software Subscriptions	Commit to an OpEx model of purchasing internal tools such as Adobe for Professional and Creative Cloud.	Intelligent Apps and Analytics

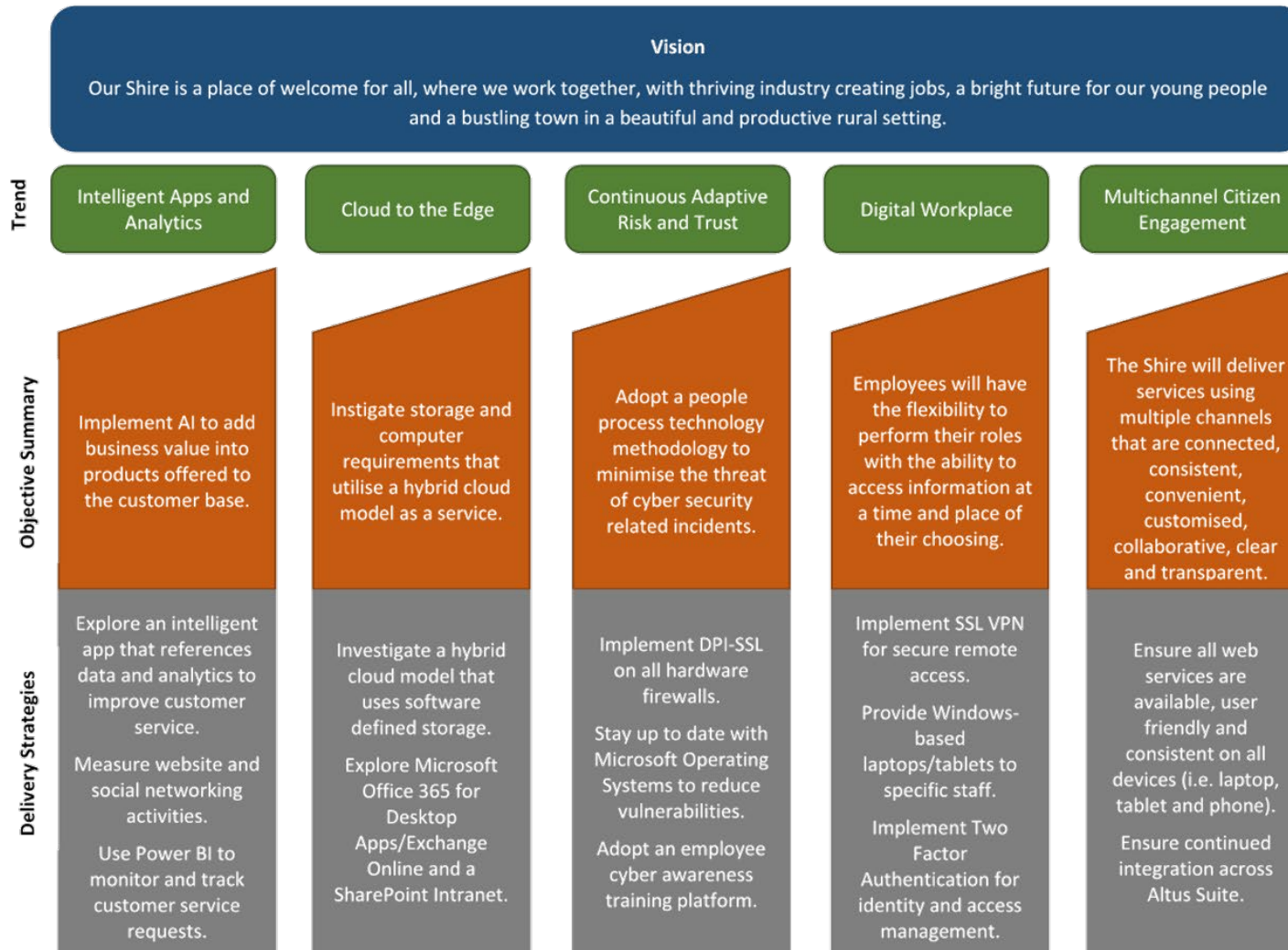
**SECTION FOUR: ICT TRENDS FOR ORGANISATIONS**

Trends and technologies in the IT industry change at an alarming rate. The Shire of Quairading is strongly reliant on day-to-day IT resources for nearly all facets of operation. As such, it is prudent to review and adopt the current industry trends for organisations (Gartner Inc.).

ICT Trend	Explanation
Intelligent Apps and Analytics	<p>Over the next few years, virtually every app, application and service will incorporate some level of AI. Some of these apps will be obvious intelligent apps that could not exist without AI and machine learning.</p> <p>AI has become the next major battleground in a wide range of software and service markets, including aspects of enterprise resource planning (ERP). Packaged software and service providers should outline how they'll be using AI to add business value in new versions in the form of advanced analytics, intelligent processes and advanced user experiences.</p>
Cloud to Edge	<p>Edge computing describes a computing topology in which information processing, and content collection and delivery, are placed closer to the sources of this information. Connectivity and latency challenges, bandwidth constraints and greater functionality embedded at the edge favours distributed models.</p> <p>While many view cloud and edge as competing approaches, cloud is a style of computing where elastically scalable technology capabilities are delivered as a service and does not inherently mandate a centralised model.</p>
Continuous Adaptive Risk and Trust	<p>To securely enable digital business initiatives in a world of advanced, targeted attacks, security and risk management leaders must adopt a continuous adaptive risk and trust assessment (CARTA) approach to allow real-time, risk and trust-based decision making with adaptive responses.</p> <p>Security infrastructure must be adaptive everywhere, to embrace the opportunity — and manage the risks — that comes delivering security that moves at the speed of digital business.</p>
Digital Workplace	<p>The government workforce of the future will be populated with digitally literate employees, from frontline workers to top-level executives. The digital workplace is open, flat and democratic. It is the organisational manifestation of open government. CIOs and IT leaders must take a leadership role in building a more social, mobile, accessible and information-driven work environment.</p> <p>Adopting this trend would allow the Shire of Quairading employees to have the flexibility to perform their roles, with the ability to access information at a time and place of their choosing. Increased productivity would be achieved over time as employees gain a greater awareness of technology services available to them through effective service delivery and communication.</p>
Multichannel Citizen Engagement	<p>Government jurisdictions with multiple channels (municipal offices, physical mail correspondence, contact centres, e-government websites and mobile apps) are struggling to provide their citizens with one coherent view of the enterprise.</p> <p>A multichannel strategy, in the context of digital government, means more than delivering a seamless experience to stakeholders. It also is about delivering</p>

<b>ICT Trend</b>	<b>Explanation</b>
	interactions that are connected, consistent, convenient, collaborative, customized, clear and transparent. To produce those outcomes, policymakers and CIOs must radically redesign service models by combining traditional marketing tools (such as focus groups, user experience labs, surveys and stakeholder analysis) with new approaches (such as citizen co-creation initiatives, agile development and design thinking).

Trend Adoption Overview





## SECTION FIVE: STRATEGIC PLAN

### 1 Backups & Disaster Recovery

#### 1.1 Industry Best Practice

Gartner, IDC, Forrester & Yankee Group report that on average, IT system downtime costs between \$84,000 and \$108,000 for every hour. Additionally, it is reported that 90% of businesses that lose all their data go out of business within the following 12 months. Protection of corporate data is achieved through a complete backup and replication solution consisting of both on premise and cloud components.

The on premise component is a device that resides within the same premises as the hardware storing the majority of corporate data. This device is responsible for regular incremental backups of nominated data at intervals in accordance with the organisation's recovery point objective (RPO). Ideally, if suitable, incremental backups for an organization with normal 8am-6pm operating hours should occur every hour. This will result in 24 intra-daily backups that should be consolidated the following day into a single daily backup. Consolidations of hourly, daily and weekly backups can occur at different stages however there should be approximately 12 months of backup's stored. This device is also responsible for the replication of all incremental backups to the cloud component.

The cloud component is a device located at a secondary site that a natural calamity or man-made disaster should not be able to affect. A minimum 500km distance should be adhered to. This device receives replicated incremental backups from the on premise device and is responsible for the long term storage, organization and consolidation of the replicated incremental backups. A minimum of 12 months of data should be stored in the cloud.

#### 1.2 Current State

##### 1.2.1 Onsite Server Backups

###### **Quairading Administration Office**

The Shire of Quairading outsource the management of backup and recovery to WCS. The currently employed system consists of the following:

Server Name	Backup Technology	Job Details
SOQ-VMHOST Virtual Machines - S22DC - S22RDS - S22ECM - ALTUS	Datto	Continuous Incremental Backups Backups done Hourly M-F between 8AM and 6PM Backups done Daily Sat-Sun between 7PM and 10PM Local data retention upto 2TB local Storage Daily Backup Monitoring by WCS Daily Backup Alerts to WCS and Client Daily Backup Tested via Screenshot Boot Capture Offsite Cloud Replication Fully managed solution by WCS. No interaction required to be completed by Shire Staff.

1.2.2 Offsite Server Backups

**Quairading Administration Office**

The Shire of Quairading outsource the management of backup and recovery to WCS. The currently employed system consists of the following:

Server Name	Backup Technology	Job Details
SOQ-VMHOST Virtual Machines - S22DC - S22RDS - S22ECM - ALTUS	Datto	Continuous Incremental Backups Replication of last backup of each day to the cloud Cloud Data Retention – Unlimited upto 12 months Daily Backup Monitoring by WCS Fully managed solution by WCS. No interaction required to be completed by Shire Staff.

1.2.3 Retention Period

**Quairading Administration Office.**

The backups maintained by WCS are defined below. Onsite backups can change. Cloud doesn't.

	Number Kept Onsite	Number Kept in Cloud	Explanation
Hourly	100	-	Hourly backups for 10 days locally
Daily	14	5	Daily backups are replicated to the cloud not hourly
Weekly	4	4	-
Monthly	6	12	-

Backups allow file based recovery to previous hour on-premises or previous day in the cloud.

**1.3 Future State Recommendations**

**Quairading Administration Office.**

The current state of backups meets the needs and requirements by the Shire of Quairading.

The Shire of Quairading Disaster Recovery Plan has been created which will also dictate if the current solution meets the business requirements moving forward.

Annual Testing of the Disaster Recovery Plan is required.

**1.4 Budget Estimate**

**Quairading Administration Office**

A backup and recovery solution will be a managed service, which means all costs are monthly on-going/operational costs.

See the following table for an indication of on-going costings.

For budget purposes, the data on premise component is set to a shared 2TB.

(Pricing is currently fixed until July 2025).

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Data on premise	10010	10010	12578

## **2 Domain**

### **2.1 Industry Best Practice**

Utilisation of Microsoft Active Directory (AD) is key to centralised management of ICT networks.

Active Directory has four primary functions:

- 2.1.1 Authentication
- 2.1.2 Policy-based Administration
- 2.1.3 Security Policies for User Accounts
- 2.1.4 Directory for Publishing Shared Resources

A user can only be authenticated by a domain controller in the domain that hosts the user's account. Where possible, any application or network resource that utilises authentication for login or access should be integrated with the domain in order to use domain authentication. This reduces the amount of credentials a user is required to remember, allowing a "Single Sign-on" (SSO) environment.

Microsoft Group Policy allows ICT administrators to standardise and manage objects within a domain using policies that can be enforced. Such objects can include user accounts and computers. It is best practice for ICT policies to be created, deployed and enforced using Group Policy.

Some basic security policies that should apply to all domain user accounts include:

- 2.1.5 Password policies
- 2.1.6 Account lockout policies
- 2.1.7 Account expiry policies

Where possible, Active Directory should be utilised to publish connection information about shared resources. As an example, printer resources might be published in a domain to facilitate searches by users.

### **2.2 Current State**

#### **Quairading Administration Office**

AD is present, reasonably well-structured and up to date. Minor group policy work is used and deployed as all workstations are AzureAD Joined.

A detailed naming structure for IT equipment exists which allows administrators to see who owns the equipment based on a role name. A naming structure for user accounts exists based on a role name which is not recommended.

FSMO (Flexible Single-Master Operations) roles and DHCP used by Active Directory are not split between servers.

The internal domain name is ad.quairading.wa.gov.au with the FSMO roles running on the SOQ-S22DC Server as well as AzureADConnect to synchronise user details to M365 Cloud.

### **2.3 Future State Recommendations**

#### **Quairading Administration Office**

The following is additional configurations should be configured to meet industry best practice:

- 2.3.1 Implementation of software deployment via Intune for workstations to improve speed and reliability of new device configuration.
- 2.3.2 Improve system log retention.
- 2.3.3 Implement removable media controls.

### **2.4 Budget Estimate**

#### **Quairading Administration Office**

The majority of this work will be implemented as part of ongoing maintenance and upgrades under the IT Support MSA provided by WCS.

### **3 Antivirus**

#### **3.1 Industry Best Practice**

An anti-virus solution should include the following features:

- 3.1.1 Scheduled full system scans
- 3.1.2 Real-time scanning
- 3.1.3 Behavioural monitoring
- 3.1.4 Anti-malware component(s)

Each of these four features should be configured and enabled for all machines requiring protection from viruses and malware.

Scheduled scans should be conducted a minimum of once per week and should be completed on all servers and client machines.

Real-time scanning can impact performance of key applications, particularly those that use a database. As such, many anti-virus vendors have released white papers on real-time scanning exclusion best practices. These best practices should be followed to avoid performance degradation of key/critical systems.

Behavioural monitoring should also always be enabled to prevent the increasingly popular ransomware viruses that encrypt data. Good anti-virus applications are able to detect when software is attempting to encrypt data and will block that application before any major damage can take place.

#### **3.2 Current State**

##### **Quairading Administration Office**

All computers and servers use Microsoft Defender for Endpoint. This product includes the following enabled features:

- 3.2.1 Smart Scan
- 3.2.2 Real-Time Scan
- 3.2.3 Web Reputation
- 3.2.4 Automatic Attack Disruption
- 3.2.5 Global Threat Intelligence

Scheduled scans are enabled for the computers and servers.

Hosted email for spam, phishing and malware protection is provided by the Microsoft Defender for 365 which is bundled with Microsoft 365 Business Premium. This system works to ensure threats are detected and stopped before entering the corporate email systems.

### **3.3 Future State Recommendations**

#### **Quairading Administration Office**

The following is industry best practice:

- 3.3.1 Expand the features set of Microsoft 365 Business Premium via continuous improvement and utilization of Microsoft Secure Score.

### **3.4 Budget Estimate**

#### **Quairading Administration Office.**

This is covered under Microsoft 365 Business Premium Licensing for AV and Email Filtering.

## **4 Corporate Applications**

### **4.1 Industry Best Practice**

Due to the numerous and varied nature of corporate applications, only generalized best practices can be listed in this section. Application vendors will normally release their own best practice white papers for specific applications which should be followed where possible.

A file management system (FMS) should continue to be employed to provide easy storage for relevant corporate data. If either on premise or hosted, a FMS requiring a back-end database should utilise Microsoft SQL and access to this data should be restricted as required. An alternative to a FMS is a document management system (DMS) such as Micro Focus Content Manager or SharePoint.

Financial software should continue to be employed to provide accounting and financial management capabilities. If either on premise or hosted, financial software requiring a back-end database should utilise Microsoft SQL and access to this data should be restricted as required.

CRM software should continue to be employed to provide membership and customer based capabilities. If either on premise or hosted, CRM and access to this data should be restricted as required.

A cyber awareness training platform should be implemented to help build employee's cybersecurity skills. An automated platform should train employees at a comfortable pace appropriate to their risk profile. Options such as an online test and simulations should be included.

### **4.2 Current State**

#### **Quairading Administration Office.**

An enterprise resource planning (ERP) suite that encompasses all business areas named SynergySoft from the company ITVision has been implemented to provide easy storage, sorting and version control for relevant corporate data. They are also used to provide accounting and financial management capabilities. The current modules include Core Financials, Customer Service, Excel Integration, Payroll, Purchase Ordering, Purchase Requisitions/Extended Security, Rates and Property including Model & Pools, Receipting, Report Manager and Stores. SynergySoft utilises an IBM U2 Universal database for the back-end database and a customized published application for the front-end interface.



Record keeping has been upgraded with the implementation of Altus ECM. This runs internally on a separate dedicated server running an SQL Database.

The SynergySoft licenses have been listed in Appendix D.

#### **4.3 Future State Recommendations**

##### **Quairading Administration Office.**

The current state meets most requirements although the development of a four-year road map is required to outline the logical transition from SynergySoft to Altus. As part of this journey which would be module by module, it would be appropriate to go to market for possible “best of breed” alternatives.

The Shire of Quairading is moving forward (very slowly currently) with the migration to Altus. This has been significantly delayed with the failure to implement Altus Payroll in the planning timeframe. This then calls into question the ability to move to full Altus Financials in the planning timeframe for the future.

To improve functionality and appearance on mobile devices (mobility), works should proceed with the current provider on the corporate website. Online payment options is one example.

A cyber awareness training platform should be implemented which hooks into HR. A solution that can start at any time for a new employee and that never stops is ideal. The idea is to reinforce knowledge without overwhelming the employee.

To improve workflow and productivity a project management tool like Trello or Monday could be investigated if the specific need and desire arises. With so many tools and packages available significant time and resources are required to make these work effectively.

#### **4.4 Budget Estimate**

##### **Quairading Administration Office.**

See the following table for an indication of on-going costings:

<b>Description</b>	<b>2023-2024 Costs</b>	<b>2024-2025 Costs</b>	<b>2025-2026 Costs</b>
SynergySoft Suite	35589	36835	38124
Altus Suite	40927	41231	41547
Website Development	7920	7920	7920
Adobe Creative Cloud	6000	6500	7000

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Cyber Awareness Training	3000	3500	3750

\*Pricing excludes GST and is a budget estimate only.

## **5 IT Support Arrangements**

### **5.1 Industry Best Practice**

Outsourced IT services should include the following;

- 5.1.1 Scheduled onsite support visits;
- 5.1.2 The ability to log support requests which are monitored and attended to;
- 5.1.3 Access to 24x7x365 support with tight service level agreements;
- 5.1.4 Proactive monitoring of the ICT network during business hours.

IT service providers should be vendor-certified relevant to any managed technology and have enough personnel to be able to adjust support hours in line with seasonal shifts in IT requirements.

Organisations that employ the service of third party IT support providers should regularly review the support schedule to ensure it fits the business requirements.

### **5.2 Current State**

The Shire of Quairading has contracted WCS to provide comprehensive Managed Services Support for all IT Support requirements. Centralise management, centralised ticketing, direct access to ticketing, monthly reporting are all included. Support is delivered as required with both remote and onsite services included.

The enterprise resource planning application (SynergySoft/Altus) is supported by WCS and ReadyTech.

### **5.3 Future State Recommendations**

Local governments face increasing pressure to enhance their security posture to address growing global threats. Implementing a robust security compliance framework is essential, with the Australian Cyber Security Centre's Essential 8 being a highly recommended option.

This framework, supported and continuously updated by the Australian Federal Government, is particularly suitable for small organizations. It offers a solid foundation for demonstrating commitment to security.

Remember, security is an ongoing journey, not a final destination.

A new security specific MSA has been applied in 2024-25 to address these areas

**5.4 Budget Estimate**

**Quairading Administration Office.**

See the following table for an indication of on-going costings:

<b>Description</b>	<b>2023-2024 Costs</b>	<b>2024-2025 Costs</b>	<b>2025-2026 Costs</b>
IT Support MSA	34647	35804	37594
Security MSA		16464	21168

## **6 IT Disaster Recovery Plan**

### **6.1 Industry Best Practice**

An IT Disaster Recovery Plan must set out the mitigation, preparation, warning, response and business continuity arrangements for all core IT systems.

The IT Disaster Recovery Plan must also:

- 6.1.1 Provide the information and procedures necessary to
  - 6.1.1.1 Respond to an occurrence
  - 6.1.1.2 Notify personnel
  - 6.1.1.3 Assemble recovery teams
  - 6.1.1.4 Recover data
  - 6.1.1.5 Resume processing at the current or alternate site as soon as possible after a disaster has been declared
- 6.1.2 Create a disaster recovery structure strong enough to provide guidance to all interrelated groups, yet flexible enough to allow staff and teams to respond to whatever type of disaster may occur.
- 6.1.3 Identify those activities necessary to resume full services at the reconstructed disaster site or new permanent facility.
- 6.1.4 Establish a return to a “business as usual” environment.

Continual review of the IT Disaster Recovery Plan should occur annually – or with significant business change – with the aim to improve existing resilience against damage to the business in the event of an actual disaster or outage.

### **6.2 Current State**

The Shire of Quairading currently has an IT Disaster Recovery Plan. This plan should be reviewed, updated and fully tested as least annually.

### **6.3 Future State Recommendations**

Continuous development and upgrade to the IT DR Plan and annual testing.

Reviewing requirements that might change in the future.

**6.4 Budget Estimate**

**Quairading Administration Office**

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
IT DR Plan Refresh (QAO)	2495	2495	2495

## **7 Internet Gateway**

### **7.1 Industry Best Practice**

A business grade internet gateway must be capable of providing advanced security services in addition to standard routing and port forwarding functionality.

Examples of advanced security services include:

- 7.1.1 Gateway Antivirus
- 7.1.2 Gateway Antispyware
- 7.1.3 Intrusion Prevention
- 7.1.4 Application Intelligence and Control
- 7.1.5 Web/Content Filtering
- 7.1.6 DPI SSL Scanning

These services deliver intelligent, real-time network security protection against the latest blended threats, including viruses, spyware, worms, Trojans, software vulnerabilities and other malicious code.

Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity.

### **7.2 Current State**

#### **Quairading Administration Office**

The Shire Administration Office currently has a Sophos XGS126 UTM Firewall which has been implemented and meets these requirements and recommendations. This is also connected Teltonika 4G Failover Internet. The primary internet connection is via CrispWireless PtP Wireless.

The Sophos UTM is managed via Cloud Access and monitored on a daily basis.

The Sophos UTM is provided via Managed Infrastructure as a Service.

#### **Quairading Community Resource Centre**

As an Ubiquiti outdoor point-to-point wireless link exists back to the Admin Office, no Internet Gateway is used.

#### **Quairading Depot**

As an Ubiquiti outdoor point-to-point wireless link exists back to the CRC, no Internet Gateway is used.

**7.3 Future State Recommendations**

**Quairading Administration Office**

The new Sophos Firewall solution has been implemented but there are always improvements that are being made.

Continuous development and implementation of the last software and features needs to continue to occur.

From time to time a review needs to be undertaken to ensure that the current hardware firewall offers the best value for the Shire.

**7.4 Budget Estimate**

**Quairading Administration Office.**

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Admin Office	2280	2280	2575

\*Pricing excludes GST and is a budget estimate only.



## **8 ISP Links**

### **8.1 Industry Best Practice**

Industry best practices dictate most organisation's IT infrastructure should have a measure of redundancy to as many components as possible – including (and especially) connections to the Internet.

A business grade Internet connection suitable for the Shire of Quairading should have the following characteristics:

- 8.1.1 Provided by a Tier 1 or 2 ISP
- 8.1.2 Guaranteed bandwidth of at least 100Mbps (preferred 100Mbps or higher at main office)
- 8.1.3 100Mbps (preferred 250Mbps) for a full cloud/hosted platform
- 8.1.4 Guaranteed contention ratio
- 8.1.5 Synchronous uplink
- 8.1.6 Delivered over fibre optic
- 8.1.7 Corporate/Enterprise level SLA

A secondary Internet connection should also be provided by a different ISP than the primary connection. The secondary connection can be a slower/lower specification service as its main function is to act as a backup connection when the primary connection fails.

In addition to failover capability, a secondary Internet connection can be utilised for load balancing. Low priority Internet services can be routed through the secondary connection to free up bandwidth from the primary connection.

### **8.2 Current State**

#### **Quairading Administration Office**

A fibre optic Internet service is too expensive as the primary Internet link. In 2022, the Shire connected all buildings to CRISP, a regional wireless provider with a wireless enterprise link (60Mbps/60Mbps).

This change has dramatically increased the reliability and performance of the IT systems. This type of bandwidth will cater for automatic offsite backups for disaster recovery, secure remote access for staff and the introduction of some hybrid cloud options.

A Telstra NextG/4G Failover service is setup and configured.

The following ISP links are currently active:

Site	Connection Type	Speed	Monthly Cost
Admin Office	CrispWireless	60Mbps/60Mbps	\$169
Admin Office	Telstra NextG	20Mbps/20Mbps	\$75

### 8.3 Future State Recommendations

#### Quairading Administration Office

The possibility of a fibre optic Internet can be reinvestigated in 2025 after the 36 month contract with CrispWireless has expired to see if there is a competitive option available.

Secondary Internet could be upgraded to Starlink Internet. The main benefit of this over current 4G connection is that if there is a major disruption like a fire or state power outage which might take out the 4G network, as we witnessed in many areas of the Wheatbelt in January 2024.

### 8.4 Budget Estimate

#### Quairading Administration Office.

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Primary Link (Wireless)	2028	2028	
Primary Fibre Optics			4200
Secondary Link (NextG)	900	900	
Starlink Failover Link			2028

\*Pricing excludes GST and is a budget estimate only.

## **9 Uninterruptable Power Supply**

### **9.1 Industry Best Practice**

Uninterruptable Power Supplies (commonly referred to as UPS) deliver online power quality and scalable battery runtimes for key IT infrastructure. In addition to providing clean power to IT equipment, a UPS is primarily utilised to keep expensive IT hardware powered on during a power outage.

High-grade UPS equipment should be installed to keep IT hardware in the main server rack(s) online for at least 1 hour during a power outage. If a power outage extends longer than the battery life of the UPS equipment, the UPS hardware should be set to gracefully shutdown all virtual servers prior to host hardware and other equipment losing power.

High-grade UPS equipment should also be equipped with modules to provide additional features such as environmental monitoring, network management and email notifications. High-grade UPS solutions address internal faults/outages by using a standby module. Alternatively, two units can be used to offer hardware redundancy.

Lower-grade UPS equipment should be installed in any location with network equipment such as switches, firewalls or modems and provide an uptime of at least 30 minutes in the event of a power outage.

Any UPS equipment powering core IT infrastructure should be tested annually to ensure indicated up-times are accurate.

### **9.2 Current State**

#### **Quairading Administration Office**

An Eaton 9PX 2000 RT UPS with no Extended Battery Module (EBM) is installed in the Administration Building computer room. This UPS is rated at 2000VA and power rails ensures all IT hardware in the server cabinets are powered via the UPS. This UPS will provide approximately 30 minutes uptime for the IT infrastructure in the event of a power outage.

This UPS does have the ability to communicate on the network but automatic shutdown procedures and parameters are not configured in cases of prolonged power outages. No shutdown can be automatically performed based on extreme temperature and/or humidity and no email notifications are configured.

**9.3 Future State Recommendations**

**Quairading Administration Office**

The UPS equipment partly meets the Shire of Quairading’s current requirements. An uptime test should be completed on an annual basis to ensure uptimes indicated are accurate. A failed test will confirm if new batteries are required.

As there is already an SNMP card (network management) installed, an EMP card (temperature probe) should be installed. This will deliver more control and allow the UPS to shut itself off and on based on set temperature and humidity readings.

**9.4 Budget Estimate**

Unfortunately, an existing UPS warranty cannot be extended so servicing the UPS is the cheapest alternative to replacing the UPS.

Device replacement would be scheduled for 2026/27 FY.

**Quairading Administration Office**

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
EMP Card		395	
Batteries		1250	

\*Pricing excludes GST and is a budget estimate only.

## **10 Computer Room**

### **10.1 Industry Best Practice**

The room(s) containing core IT infrastructure should have the following properties:

- 10.1.1 Independent and redundant air-conditioning
- 10.1.2 Backup ventilation fan
- 10.1.3 Dedicated 15A+ (or higher) power circuit for each UPS
- 10.1.4 Sufficient storage for IT hardware, spare cabling and software
- 10.1.5 Non-carpet flooring to minimise dust
- 10.1.6 Lockable door

In addition to the above, a desk and chair should be provided for any IT support staff that attend site if possible.

### **10.2 Current State**

#### **Quairading Administration Office**

A 28RU cabinet is located in a shared multi use storage/archive room. The room door is locked. There is a split system air conditioning installed in this room, however, this is only in use during business hours.

Data cabling is well set out and labelled correctly with ample cable management. Most communications equipment is rack mounted although the UPS which is designed to be rack mounted, is installed on its side with the rail kit still in the box. Unfortunately, the HPE server is not rack mounted.

#### **Quairading Community Resource Centre**

As the Community Resource Centre is a multi-tenanted building, the Shire of Quairading equipment is located in a wall-mounted cabinet in the storeroom. This wall-mounted cabinet contains equipment for all tenants making it less secure.

*Data cabling is messy as no cable management is used.*

#### **Quairading Depot**

Quairading Depot was upgrading with a new rack at the end of 2022. Data cabling is well managed and fully documented.

### **10.3 Future State Recommendations**

#### **Quairading Administration Office**

The shared multi use storage/archive room means the door to this room cannot change and must stay locked at all times with the key documented and stored safely.

The door to the right hand side of the cabinet must be re-installed and the key to the cabinet documented and stored safely.

The replacement server is rack mounted and cabling has been improved in 2022.

#### **Quairading Community Resource Centre**

As the Community Resource Centre is a multi-tenanted building, it is very difficult to segregate the equipment for all tenants.

As the data cabling is messy and no cable management is used, shorter CAT6a cables should be used to help make the install cleaner and easier to fault find.

Documentation needs to be updated with Visio Maps created for better remote support options.

#### **Quairading Depot**

No further changes are required for this.

### **10.4 Budget Estimate**

#### **Quairading Community Resource Centre**

See the following table for an indication of on-going costings:

<b>Description</b>	<b>2023-2024 Costs</b>	<b>2024-2025 Costs</b>	<b>2025-2026 Costs</b>
Supply CAT6a Cables		500	
Project Labour		2500	

## **11 Local Area Network**

### **11.1 Industry Best Practice**

Core network switching should provide the following:

- 11.1.1 Layer 3 routing functionality
- 11.1.2 Management interface
- 11.1.3 Power over Ethernet
- 11.1.4 At least 1000Mbps (1 gigabit) connectivity to all computers
- 11.1.5 At least 10000Mbps (10 gigabit) connectivity to all servers

Additionally, core network switching should always be configured in a redundant stack.

Local area networks should utilise VLAN encapsulation for logical segregation of network traffic.

Internal Wi-Fi access points can be configured on different frequency ranges. Each range is divided into channels. Fine tuning can increase performance gains. Wireless network access can be configured using SSIDs, VLANs and user authentication to increase security.

Public/visitor Wi-Fi networks should also be securely segregated from corporate networks via VLAN encapsulation.

### **11.2 Current State**

#### **Quairading Administration Office**

In the server rack there is a Ubiquiti USW-PRO-48-POE in the shared Multi-Use Storage/Archive room. This switch, which was upgraded in 2022, has over 25% capacity available. This switch is full Layer 3 and POE enabled.

There are currently two Ubiquiti U6 LR Wireless Access Points installed in the main office to provide full coverage and redundancy. This Wi-Fi network is the corporate network it has a segregated guest network for visitors.

#### **Quairading Community Resource Centre**

There is a Ubiquiti USW-PRO-24 switch rack mounted inside the wall-mounted cabinet in the Community Resource Centre storeroom. 18 of the 24 ports are free so there is plenty of space available for expansion. NOTE: This is not POE Enabled.

There is no Wi-Fi provided by the Shire.

**Quairading Depot**

There has been a Ubiquiti USW-PRO-24-POE installed in the new comms rack at the Depot. This is a 24 port Layer 3 switch and this currently has 6 ports available.

Internal Wi-Fi is delivered through multiple Ubiquiti AP AC-Pro. This Wi-Fi network is the corporate network it has a segregated guest network for visitors.

**11.3 Future State Recommendations**

**All Commercial Shire Buildings**

To address current and future security requirements, standardised on networking equipment needs to be purchased as the network is expanded and upgraded.

Ongoing management and performance monitoring of network to ensure smooth and efficient operations for all staff members. This is across wireless, wireless and ptp networks.

Review security configuration of the network on a regularly basis to see if there are any improvements that can be implemented.

**11.4 Budget Estimate**

**Quairading Administration Office**

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
EAP Security Configurations		1500	

\*Pricing excludes GST and is a budget estimate only.



## **12 Desktops / Laptops**

### **12.1 Industry Best Practice**

Standard IT practices and return on investment analysis from Industry bodies such as Gartner Group dictate a three-year lifecycle for standard business desktops. These industry standards are reflected by the tier one companies such as HP, Lenovo and DELL who generally ship such machines with a standard three-year onsite warranty.

A replacement business desktop should be obtained from a tier one vendor such as Dell, HP or Lenovo who have a three-year hardware life cycle. This ensures a small number of Standard Operating Environment's (SOE) can be maintained across the three-year desktop lifecycle.

A shift away from small form factor desktop machines to "mini desktop" frees up office desk space for all staff. These machines are also more energy efficient and have silent operation.

A true business laptop will ensure standard accessories including docking stations, and extended batteries are available.

### **12.2 Current State**

#### **Quairading Administration Office, Community Resource Centre & Depot**

The Shire of Quairading currently utilise a majority of business/enterprise computers systems primarily from Lenovo, Dynabook and Dell. The fleet numbers approximately 30 computers.

Windows 10/11 Business & Microsoft 365 Business Premium have been deployed thru Intune.

Windows updates for computers and servers is managed by Wallis Computer Solutions

Third-party patching (Java, Adobe, Flash etc.) has been implemented by Wallis Computer Solutions.

### **12.3 Future State Recommendations**

#### **Quairading Administration Office, Community Resource Centre & Depot**

The Shire will be standardising the purchasing of computers. In an ideal world one manufacturer is chosen which can reduce the overheads involved with managing a fleet of computers from a driver/support point of view. Bulk purchasing of computers can lead to discounted pricing. The purchasing of computers can be staggered across multiple years so that the fleet is refreshed

regularly without requiring a big capex investment. The Shire will compare the leasing model with outright purchasing during the next computer purchase.

Staff will be given a mini desktop if they never leave the office or require a fixed desktop setup.

Customer facing front office staff are an example of this. To increase mobility and productivity, key staff should be supplied a laptop with accessories such as a docking station and two LCD screens. The laptop is taken home to be securely used remotely and placed back into the docking station when in the office. Most importantly, every user should only have one computer.

The Shire will research implementing an SOE which would include Windows 11 Professional with Office 365. A migration to Office 365 has been completed in 2022. Office 365 will provide additional capabilities such as Microsoft Teams and SharePoint Online.

Please refer to Appendix A for a complete list of desktop/laptop hardware replacements and relevant information.

**Budget Estimate**

Description	Current Replacement Costs
Desktop Mini with Accessories and Screens	2000
Business Laptop with Accessories and Screens	2750
Business Tablet with Accessories and Screens	3500

**Quairading Administration Office, Community Resource Centre & Depot**

See the following table for an indication of on-going costings. These costings are excluding related project labour:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Desktop Mini	4000	2000	2000
Business Laptop	5500	8250	8250
Business Tablet	7000	7000	7000
Office 365	15018	15985	16865

\*Pricing excludes GST and is a budget estimate only.

### 13 Servers

#### 13.1 Industry Best Practice

Physical server hardware should be specified which supports a virtual server environment, to provide the best possible return on investment on server hardware via increased utilisation. If uptime is essential the N+1 architecture delivers a minimum of two physical servers using a software defined storage solution.

The greater IT Industry has observed a large shift to virtual server environments, which started nearly a decade ago in the enterprise market space. This trend has migrated rapidly down to the small to medium business in recent times as vendors target their pricing and products towards this more price sensitive end of the market.

Current offerings of server hardware provide significant excess performance capability which can be employed to support multiple simultaneous servers on the one server. This approach makes the best use of expensive server hardware, allows effective management of shared server storage and can be leveraged to reduce downtime.

Physical server hardware should employ as many redundancy options as possible, such as:

- 13.1.1 Redundant power supplies
- 13.1.2 Redundant cooling
- 13.1.3 Redundant 10GB network connectivity
- 13.1.4 Redundant hard drive configurations (RAID5 + hot spare disks)

Virtual servers should be built to a Windows Server 2019 standard as a minimum.

#### 13.2 Current State Recommendations

##### Quairading Administration Office

A Server Migration/Replacement with Dell PowerEdge R540 Server and Migration to O365 has occurred in 2022 and this comes with a 7 year ProSupport Warranty (Expiring 2029)

#### 13.3 Budget Estimate

##### Quairading Administration Office

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Server Replacements			

## **14 Storage**

### **14.1 Industry Best Practice**

Two common forms of storage exist being SAN hardware or local disk server storage.

SAN hardware should always be capable of easy expansion for future data requirements, by allowing additional hard drives and hard drive shelves to be installed. This flexibility will ensure a major upgrade to server infrastructure will not be required in the standard server/SAN life cycle. The SAN is one of the most vital components of the IT infrastructure and therefore should employ as many redundancy options as possible, such as:

- 14.1.1 Redundant storage processors
- 14.1.2 Redundant power supplies
- 14.1.3 Redundant cooling
- 14.1.4 Redundant 10GB network connectivity
- 14.1.5 Redundant hard drive configurations (RAID5 + hot spare disks)

Local disk server storage should always be capable of easy expansion for future data requirements, by allowing additional hard drives to be installed. Local disk server storage should employ redundancy options such as:

- 14.1.6 Redundant hard drive configurations (RAID5 + hot spare disks)
- 14.1.7 Software defined storage solution (two or more physical servers)

### **14.2 Current State**

#### **Quairading Administration Office**

The Shire of Quairading Dell R550 meets all requirements although it is server vs specific SAN.

### **14.3 Future State Recommendations**

#### **Quairading Administration Office**

The Shire of Quairading Dell R550 meets all requirements with warranty due for expiry in 2029.

### **14.4 Budget Estimate**

#### **Quairading Administration Office**

The Shire of Quairading Dell R550 meets all requirements and no additional costs for the foreseeable future.

**15 IP Telephony**

**15.1 Industry Best Practice**

IP Telephony is the technology that makes it possible to have telephone conversations over the Internet or a dedicated IP network (instead of dedicated voice transmission lines).

A dedicated IP network should be utilised in order to guarantee quality, as voice calls over the Internet take a “best effort” approach, which can result in poor or degraded quality.

Consideration should be given for a VOIP PABX, which allows for control and configuration of the telephony system by internal staff or contracted support staff.

Client computers should be connected to the local area network via the associated VOIP phone handset, therefore all VOIP phone handsets should allow gigabit connectivity to the network. This approach reduces switching and cabling costs.

**15.2 Current State Recommendations**

**Quairading Administration Office & Medical Clinic**

A 3CX VoIP Phone System has been deployed for both Administration Office and Medical Clinic. Services have been migrated to the new carrier with the ability for remote access, call routing between locations, voicemail and remote provisioning of devices.

This is all setup, configured, managed by Wallis Computer Solutions.

This is a fixed price 60 month agreement including handsets, calls and support.

This system is scalable and can increase in handsets as required by the Shire.

**15.3 Budget Estimates**

**Quairading Administration Office & Medical Clinic**

See the following table for an indication of on-going costings:

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
3CX Phone System	12210	12420	12630

## **16 Printing**

### **16.1 Industry Best Practice**

Printing is one of the most critical functions of an IT system and consequently can be one of the most frustrating when not setup correctly. One or two large duty cycle multifunction copiers should be deployed on each floor or central location within the main office. Printer drivers should be deployed utilising universal drivers where possible, via Microsoft group policy.

Where required, additional printers can be deployed, however these should always be laser printers, sourced from a Tier 1 vendor and capable of connecting to the local area network.

The printing technology should also be capable of providing a “secure print” feature, which prevents documents from being physically printed, until a staff member logs into the printer and “releases” the print job. This allows for secure and confidential printing in a centralised printing environment.

### **16.2 Current State**

#### **Quairading Administration Office**

Centralised printing has been implemented using a mixture of printers with the Canon iR-ADV 7765 being the central multi-function printer. Secure Print has not been implemented.

One smaller HP LaserJet printers are also in operation.

A Kyocera M4132idn has been deployed in 2023 to the Depot.

#### **Future State Recommendations**

##### **Quairading Administration Office**

The Canon C7765 has its final payment due in May 2024.

It is expected that it will be replaced in 2024-25 Financial Year, most likely on a lease for something with a similar cost.

The depot printer installed in 2023 should be fine for ~ 5 Years. So replacement should be planned for around 2028.

**16.3 Budget Estimates**

**Quairading Administration Office**

See the following table for an indication of on-going costings.

Depot printer was purchased and Office Photocopier is leased over 60 months.

Description	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Depot MFP Purchase	3729		
Office Photocopier Lease	3390	3390	3390

\*Pricing excludes GST and is a budget estimate only.

APPENDIX A: WORKSTATIONS / TABLETS / LAPTOPS

Agent Name	Agent Type	Agent Manufacturer	Agent Mainboard	Windows Version	Agent User	Agent Serial Number	Purchased
SOQ-WS2WX64	WorkStation	HP	HP EliteDesk 800 G3 SFF	Windows 10 Pro	SOQ\jason.mashford	AUD7320BNG	17/18
SOQ-WS3WX64	WorkStation	HP	HP EliteDesk 800 G3 SFF	Windows 10 Pro	SOQ\debra.matthews	AUD8070FY9	17/18
SOQ-LP6WXI	Laptop	LENOVO	81YE	Windows 10 Pro	SOQ\sarah.caporn	PF271AF6	18/19
SOQ-LP10WXI	Laptop	Acer	TravelMate P215-52	Windows 10 Pro	SOQ\jason.lilleyman	03800343	19/20
SOQ-LP11WX64	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\cynthia.yarran	PF2N03MJ	19/20
SOQ-LP12WX64	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\chambers	PF2MXDVL	19/20
SOQ-LP13WX64	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\tricia.brown	PF2MXDTZ	19/20
SOQ-LP14WX64	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\Chambers	PF2M2ZJ3	19/20
SOQ-LP15WXI	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\jason.mashford	PF2MZFRN	19/20
SOQ-LP16WX64	Laptop	LENOVO	82C5	Windows 10 Pro	SOQ\wrf	PF2MZN0Y	19/20
SOQ-LP1WX64	Laptop	ASUS	X541UAK	Windows 10 Pro	AzureAD\Quairading-Managerof	H4N0CX15D55817D	19/20
SOQ-LP7WX64	Laptop	ASUS	ZenBook UX362FA_UX362FA	Windows 10 Pro	SOQ\Nicole.Gibbs	KCN0CV01200349B	19/20
SOQ-LP8WX64	Laptop	ASUS	ZenBook UX362FA_UX362FA	Windows 10 Pro	SOQ\cynthia.lowe	KCN0CV012020499	19/20
SOQ-LP17WX64	Laptop	ASUS	ZenBook UX363EA_UX363EA	Windows 10 Pro	SOQ\dean.mastin	LBN0CX13U131479	21/22
SOQ-LP18WXI	Laptop	LENOVO	82KB	Windows 11 Pro	SOQ\josh.thompson	PF39V8JX	21/22



Agent Name	Agent Type	Agent Manufacturer	Agent Mainboard	Windows Version	Agent User	Agent Serial Number	Purchased
SOQ-LP19WXI	Laptop	Acer	Extensa 215-54	Windows 11 Pro	SOQ\morganne.brunsdon	NXEGJSA0022110BE0C3400	21/22
SOQ-LP22WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	CrHayes	5KMVMG3	21/22
SOQ-LP24WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ-LP24WXI\crhippisle	9KMVMG3	21/22
SOQ-LP25WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ\soqadmin	4KMVMG3	21/22
SOQ-LP26WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ-LP26WXI\crstacey	3KMVMG3	21/22
SOQ-LP28WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ-LP28WXI\crcowcill	4TXRMG3	21/22
SOQ-LP29WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	CrCheang	6KMVMG3	21/22
SOQ-LP30WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ-LP30WXI\crsmith	7KMVMG3	21/22
SOQ-LP31WXI	Laptop	Dell	Inspiron 7506 2n1	Windows 11 Pro	SOQ-LP31WXI\crhaythornthwaite	6LZRMG3	21/22
SOQ-LP27WX64	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\natalie.ness	92136246H	22/23
SOQ-LP33WX	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\chloe.nella	33079476H	22/23
SOQ-LP34WX	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\marion.haeusler	33079738H	22/23
SOQ-WS32WX	WorkStation	EDsys Computers	EDAIOI5245	Windows 11 Pro	SOQ-WS32WX\Library	B349723	22/23
SOQ-LP35WXI	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\dean.mastin	63100709H	23/24
SOQ-LP36WXI	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\sarah.caporn	63107966H	23/24
SOQ-LP37WXI	Laptop	Dynabook Inc.	TECRA A50-K	Windows 11 Pro	SOQ\tricia.brown	34084233H	23/24

**APPENDIX B: PRINTERS**

**Quairading Administration Office.**

<b>Printer Name</b>	<b>Make</b>	<b>Model</b>	<b>Serial No</b>	<b>Location</b>	<b>IP Address</b>	<b>Date Purchased</b>
SOQ-OFF-PRT1	Canon	iR-ADV C7765	5C25653 I R	Administration Building	172.20.61.40	2017-18 Replace: 2024-25
SOQ-OFF-PRT2	HP	M2235dn		Administration Building	172.20.61.41	~2015
SOQ-DEP-PRT3	Kyocera	Ecosys M4132idn	CN79M6507C	Depot	172.20.61.42	2022-23

**APPENDIX C: MICROSOFT LICENSES**

**Quairading Administration Office.**

<b>Part No</b>	<b>Product Description</b>	<b>Qty Ordered</b>	<b>Coverage Period</b>
	Server 2022 Standard 16 Core	2	Perpetual
	Server 2022 User CALs	32	Perpetual
	Server 2022 Remote Desktop Services – User CAL	29	Perpetual
	SQL Server 2019 Standard	1	Perpetual
	SQL Server 2019 User CALs	29	Perpetual
	WCS O365 Administrative Bundle	1	Annual
	Microsoft 365 Business Basics + EOA	7	Annual
	Microsoft 365 Business Premium	30	Annual
	Microsoft 365 Defender for Server	5	Annual

APPENDIX D: ADDITIONAL LICENSES – SYNERGYSOFT AND ALTUS

Cost	2022/23	2023/24	2024/25	2025/26	2026/27
Annual licence fee (existing)	\$22,924	\$23,726*	\$24,557*	\$25,416*	\$26,306*
50% uplift	\$11,462	\$11,863*	\$12,278*	\$12,708*	\$13,153*
Altus Payroll licence fee	\$8,400	\$8,694*	\$8,998*	\$9,313*	\$9,639*
Altus Payroll implementation	\$49,883				
Module Implementation Costs (Smoothed)		\$32,233	\$32,233	\$32,233	\$32,233
<b>Total investment</b>	<b>\$92,669</b>	<b>\$76,517</b>	<b>\$78,066</b>	<b>\$79,671</b>	<b>\$81,331</b>

\* Includes CPI estimate increase at 3.5% per annum

APPENDIX E: SUMMARY OF ESTIMATES

Quairading Administration Office/CRC/Depot.

Category	Description	Priority Number	Dependency Category	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
5.1	Backup & Disaster Recovery	1	5.1, 5.6, 5.7, 5.8	10010	10010	12578
5.2	Domain	4		0	0	0
5.3	Anti-Virus	11		0	0	0
5.4	Corporate Applications	7		93427	95986	98341
5.5	IT Support Arrangement	8		34647	51111	55815
5.6	IT Disaster Recovery Plan	2	5.1	2495	2495	2495
5.7	Internet Gateway	3	5.8	2280	2280	2580
5.8	ISP Links	5	5.7	2928	2928	6228
5.9	Uninterrupted Power Supply	13			1645	
5.10	Computer Room	16			3000	
5.11	Local Area Network	12			1500	
5.12	Desktop / Laptops	6		31518	33235	34115
5.13	Servers	9	5.14	0	0	0
5.14	Storage*	10	5.13	0	0	0
5.15	IP Telephony	14		8712	12420	12630
5.16	Printing	15		7119	3390	3390
	MINOR EQUIPMENT					
	<b>TOTAL</b>					

The Priority Number suggests the importance of the change. 1 represents a high priority i.e. now and 16 represents a low priority.

The Dependency Category shows a link between the categories. A link means other categories are required to complete the task.

\* The costs associated with 5.14 Storage are incurred within the 5.13 Server item due to Server and Storage being the same hardware.

## GLOSSARY OF TERMS

### **3DES**

Triple DES is a mode of the DES encryption algorithm that encrypts data three times. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key).

### **4G**

4G is the fourth generation of wireless mobile telecommunications technology, succeeding 3G. Potential and current applications include amended mobile web access, IP telephony, gaming services, high-definition mobile TV, video conferencing, and 3D television

### **Active Directory**

Active Directory (AD) is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was only in charge of centralized domain management. Starting with Windows Server 2008, however, Active Directory became an umbrella title for a broad range of directory-based identity-related services.

### **ADSL**

(Asymmetric Digital Subscriber Line) is a technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. ADSL is an asynchronous service that delivers a faster download speed but slower upload speed.

### **AES**

Advanced Encryption Standard (AES) is an encryption algorithm for securing sensitive but unclassified material by U.S. Government agencies and, as a likely consequence, may eventually become the de facto encryption standard for commercial transactions in the private sector.

### **BDSL**

(Broadband or Business Digital Subscriber Line) is a technology for transmitting digital information at a high bandwidth on existing phone lines to homes and businesses. Unlike ADSL, BDSL is a synchronous service that delivers the same download and upload speeds.

#### **CAL**

A Client Access License (CAL) is a license granting access to certain Microsoft server software. CALs are used in conjunction with Microsoft Server software licenses to allow Users and Devices to access and utilise the services of that server software.

#### **Cat5**

ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. Cat5 supports data rates of 100 Mbps or 1000 Mbps (4 pair).

#### **Cat6**

ANSI/EIA (American National Standards Institute/Electronic Industries Association) Standard 568 is one of several standards that specify "categories" (the singular is commonly referred to as "CAT") of twisted pair cabling systems (wires, junctions, and connectors) in terms of the data rates that they can sustain. Cat6 supports data rates of 1000 Mbps (1Gbps) or 10000 Mbps (10Gbps).

#### **Cloud Computing**

A type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling ubiquitous, on-demand access to a shared pool of configurable computing resources which can be rapidly provisioned and released with minimal management effort.

#### **CMS**

A content management system (CMS) is a computer application that supports the creation and modification of digital content using a simple interface to abstract away low-level details unless required, usually supporting multiple users working in a collaborative environment.

#### **CPU**

A central processing unit (CPU) is the electronic circuitry within a computer that carries out the instructions of a computer program by performing the basic arithmetic, logical, control and input/output (I/O) operations specified by the instructions.

### **CRM**

Customer relationship management (CRM) is a term that refers to practices, strategies and technologies that companies use to manage and analyze customer interactions and data throughout the customer lifecycle, with the goal of improving business relationships with customers.

### **Deep Packet Inspection**

Deep packet inspection (DPI) is a technology which allows a firewall device to classify passing traffic based on rules that not only include information about layer 3 and layer 4 contents of the packet, but also include information that describes the contents of the packet's payload – including the application data (for example, an FTP session, or a HTTP Web browser session, or even a middleware database connection).

### **DHCP**

Dynamic Host Configuration Protocol (DHCP) is a communications protocol that lets network administrators manage centrally and automate the assignment of Internet Protocol (IP) addresses in an organisation's network.

### **DNS**

The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses.

### **Domain**

A domain name is an identification string that defines a realm of administrative autonomy, authority, or control on the Internet. Domain names are formed by the rules and procedures of the Domain Name System (DNS). Domain names are used in various networking contexts and application-specific naming and addressing purposes.

### **Disaster Recovery**

Disaster recovery (DR) involves a set of policies and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. Disaster recovery focuses on the IT or technology systems supporting critical business functions.

### **EDRMS**

Electronic document and records management system (EDRMS) is a type of content management system and refers to the combined technologies of document management and records management systems as an integrated system.



### **EMC**

EMC is a leading provider of IT storage hardware solutions to promote data backup and recovery and accelerate the journey to cloud computing.

### **ESXi**

ESX Server is VMware's flagship enterprise server virtualization platform. It comes in two versions – ESX Server and ESXi Server where the latter has no service console and is the thinnest version available. ESX is an enterprise-level product developed by VMware Inc. that is used for server virtualization.

### **Ethernet**

Ethernet is the most widely installed local area network LAN technology. An Ethernet LAN used to use coaxial cable but these days uses special grades of twisted pair wires.

### **Fibre**

An optical fibre is a flexible, transparent fibre made by drawing glass (silica) or plastic to a diameter slightly thicker than that of a human hair. Optical fibres are used most often as a means to transmit light between the two ends of the fibre and find wide usage in fibre-optic communications, where they permit transmission over longer distances and at higher bandwidths (data rates) than wire cables.

### **Firewall**

A firewall is a set of related programs, located at a network gateway that protects the resources of a private network from users from other networks. The term also implies the security policy that is used with the programs.

### **FSMO**

FSMO is a specialized domain controller (DC) set of tasks, used where standard data transfer and update methods are inadequate. Active Directory (AD) normally relies on multiple peer DCs, each with a copy of the AD database, being synchronized by multi-master replication.

### **FTP**

File Transfer Protocol (FTP) is a standard Internet protocol. It is arguably the simplest way to exchange files between computers on the Internet. It is also commonly used to download programs and other files to your computer from other servers.

#### **GAS**

Gateway anti-spyware (GAS) is a signature-based security solution that provides dynamic spyware protection at the perimeter of your network. The service blocks the installation of malicious spyware at the gateway and disrupts background communications from existing spyware programs that transmit confidential data.

#### **GAV**

Gateway anti-virus (GAV) is a signature-based security solution that provides protection at the perimeter of your network. They are your first line of defense, scanning inbound and outbound traffic to identify and block malicious threats before they can enter your network.

#### **GIS**

A geographic information system (**GIS**) is a computer system for capturing, storing, checking, and displaying data related to positions on Earth's surface. **GIS** can show many different kinds of data on one map. This enables people to more easily see, analyze, and understand patterns and relationships.

#### **Group Policy**

Group Policy is a feature of the Microsoft Windows NT family of operating systems that controls the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

#### **GWIP**

Government Wideband Internet Protocol (GWIP) is a uniquely flexible, high-speed data networking solution that offers a simple cost-effective means of interconnecting offices throughout Australia.

#### **HDD**

A hard disk drive (HDD), hard disk, hard drive or fixed disk is a data storage device used for storing and retrieving digital information using one or more rigid rapidly rotating disks (platters) coated with magnetic material.

#### **Hybrid cloud**

A composition of two or more clouds (private, community or public) that remain distinct entities but are bound together, offering the benefits of multiple deployment models. Hybrid cloud can also mean the ability to connect collocation, managed and/or dedicated services with cloud resources.

## **ICT**

Information and communications technology (ICT) is an extended term for information technology (IT) which stresses the role of unified communication and the integration of telecommunications (telephone lines and wireless signals), computers as well as necessary enterprise software, middleware, storage, and audio-visual systems, which enable users to access, store, transmit, and manipulate information.

## **IP Address**

An IP address is a 32-bit number that identifies each sender or receiver of information that is sent in packets across the network or Internet. The IP address has two parts: the identifier of a particular network on the Internet and an identifier of the particular device within that network. Due to the enormous growth of the Internet and the predicted depletion of available addresses, a new addressing system (IPv6), using 128 bits for the address, was developed in 1995.

## **IPS**

Intrusion Prevention Service (IPS) is a pre-emptive approach to network security used to identify potential threats and respond to them swiftly. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator.

## **IPsec**

A suite of protocols defining the security services developed by the Internet Engineering Task Force (IETF). IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks.

## **ISP**

An ISP (Internet service provider) is a company that provides individuals and other companies' access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served.

## **HA Pair**

Some SonicWALL Firewall devices can be configured as a High-availability pair (HA Pair) which allows the primary and backup firewall devices to continuously synchronise so that the backup unit can seamlessly assume all network responsibilities should the primary unit fail.

### **HTTP**

The Hypertext Transfer Protocol (HTTP) is the set of rules for exchanging files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. By default, HTTP operates on port 80.

### **LAN**

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

### **Load Balancing**

Load balancing allows the enabling of an interface as a secondary WAN port. The primary and secondary WAN ports are used in a more dynamic active/active setup, where the outbound traffic is divided to flow out between the primary WAN port and the secondary WAN port.

### **LRM**

Limited Retirement Mode (LRM) is an announcement by Dell SonicWALL to indicate that it will no longer develop or release firmware updates or new features for these products. Software and firmware support for products in LRM is limited to critical bugs and security vulnerabilities.

### **LTO**

Linear Tape-Open (LTO) is an open-format tape storage technology developed by Hewlett-Packard (HP), International Business Machines (IBM), and Certance. The term "open-format" means that users have access to multiple sources of storage media products that will be compatible. The high-capacity implementation of LTO technology is known as the LTO Ultrium format, or simply LTO Ultrium.

### **Malware**

Malware (for "malicious software") is any program or file that is harmful to a computer user. Thus, malware includes computer viruses, worms, Trojans, and also spyware, programming that gathers information about a computer user without permission.

### **Mbps**

Mbps stands for millions of bits per second or megabits per second and is a measure of bandwidth (the total information flow over a given time) on a telecommunications medium. Depending on the medium and the transmission method, bandwidth is also sometimes measured in the Kbps (thousands of bits or kilobits per second) range or the Gbps (billions of bits or gigabits per second) range.

### **MTO**

The maximum tolerable outage is the amount of time the critical business functions may be without the support of IT systems and applications before business operations are severely impacted. The MTO encompasses all activities from point of impact to point of recovery.

### **NAS**

Network-attached storage (NAS) is a file-level computer data storage server connected to a computer network providing data access to a heterogeneous group of clients. NAS is specialised for serving files either by its hardware, software, or configuration. It is often manufactured as a computer appliance – a purpose-built specialised computer.

### **NAT**

Network Address Translation (NAT) is the translation of an Internet Protocol address IP Address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

### **NBN**

The National Broadband Network (NBN) is an Australian national wholesale-only, open-access data network. It is based on the premise that access to fixed line, wireless and satellite broadband connections are sold to retail service providers (RSPs), who then sell internet access and other services to consumers.

### **NSA**

Dell SonicWALL Network Security Appliance (NSA) Series firewall's offer high-performance security against an array of attacks. The NSA Series combines Dell's patented Reassembly-Free Deep Packet Inspection (RFDPI) single-pass threat prevention engine with a powerful, scalable multi-core architecture.

### **NTFS**

NT File System (sometimes New Technology File System) is the file system that the Windows NT operating system uses for storing and retrieving files on a hard disk. NTFS is the Windows NT equivalent of the Windows 95 file allocation table (FAT) and the OS/2 High Performance File System (HPFS).

### **On-premises**

Software is installed and runs on computers on the premises (in the building) rather than at a remote facility such as a server farm or cloud. On-premises software is sometimes referred to as "shrinkwrap" software, and off-premises software is commonly called "software as a service".

### **PoE**

Power over Ethernet (PoE) is the process of transmitting power to the target device at the end of an Ethernet cable by carrying power in the unused 4/5 and 7/8 wires. It enables access points and other remote devices to be installed where there is no power outlet.

### **Port**

A port referred to in TCP/IP and UDP networks, is an endpoint to a logical connection. The port number identifies what type of port it is. For example, port 80 is used for HTTP traffic. Ports on a system can be left open for an incoming connection or closed to restrict unwanted access.

### **RAID**

RAID (originally redundant array of inexpensive disks, now commonly array of independent disks) is a data storage virtualization technology that combines multiple physical disk drive components into a single logical unit for the purposes of data redundancy, performance improvement, or both.

### **RAM**

Random-access memory (RAM) is a form of computer data storage. A random-access memory device allows data items to be read or written in almost the same amount of time irrespective of the physical location of data inside the memory

### **Ransomware**

A computer malware that installs covertly on a victim's computer, executes a cryptovirology attack that adversely affects it, and demands a ransom payment to restore it. Simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, and display a message requesting payment to unlock it.

### **RDP**

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection.

### **Router**

On the Internet, a router is a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination. The router is connected to at least two networks and decides which way to send each information packet based on its current understanding of the state of the networks it is connected to.

#### **RPO**

The point in time to which systems and data must be recovered after an outage (e.g., end of the previous day's processing). RPOs are often used as the basis for the development of backup strategies.

#### **RTO**

The period of time within which systems, applications or functions must be recovered after a disaster declaration (e.g. one business day). RTOs are often used to determine whether or not to implement the recovery strategies/plan.

#### **SAN**

A storage area network (SAN) is a network which provides access to consolidated, block level data storage. SANs are primarily used to enhance storage devices so that the devices appear to the operating system as locally attached devices. A SAN typically has its own network of storage devices that are generally not accessible through the local area network (LAN) by other devices.

#### **SAS**

Serial Attached SCSI (SAS) is a point-to-point serial protocol that moves data to and from computer storage devices such as hard drives and tape drives. SAS replaces the older Parallel SCSI (Small Computer System Interface, usually pronounced "scuzzy") bus technology that first appeared in the mid-1980s.

#### **SATA**

Serial ATA (SATA, abbreviated from Serial AT Attachment) is a computer bus interface that connects host bus adapters to mass storage devices such as hard disk drives, optical drives, and solid-state drives. Serial ATA succeeded the older Parallel ATA (PATA) standard, offering several advantages over the older interface: reduced cable size and cost (seven conductors instead of 40 or 80), native hot swapping, faster data transfer through higher signalling rates, and more efficient transfer through an (optional) I/O queuing protocol.

#### **SFF**

A small form factor (SFF) is a computer form factor designed to minimize the volume of a desktop computer. In some cases, this term can be used to describe physical hard disks that are smaller than the standard 3.5" hard drives.

### **SIP**

The Session Initiation Protocol (SIP) is a communications protocol for signaling and controlling multimedia communication sessions. The most common applications of SIP are in Internet telephony for voice and video calls, as well as instant messaging, over Internet Protocol (IP) networks.

### **SLA**

A service-level agreement (SLA) is a part of a standardised service contract where a service is formally defined. Particular aspects of the service – scope, quality, responsibilities – are agreed between the service provider and the service user. A common feature of an SLA is a contracted delivery time (of the service or performance).

### **SMTP**

Simple Mail Transfer Protocol is a protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. SMTP is usually implemented over Transmission Control Protocol port 25.

### **Snapshot**

In [computer systems](#), a snapshot is the [state](#) of a system at a particular point in time. The term was coined as an analogy to that in [photography](#). It can refer to an [actual copy](#) of the state of a system or to a capability provided by certain systems.

### **SNMP**

Simple Network Management Protocol (SNMP) is an "Internet-standard protocol for managing devices on IP networks. Devices that typically support SNMP include routers, switches and servers. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

### **SOE**

Standard Operating Environment is a specification for a using a standard architecture and applications within an organisation. There is no industry-wide SOE standardisation, however organisations would usually deploy standard disks, operating systems, computer hardware (with the same configurations), and standard applications and software.

### **Spyware**

Spyware is any technology that aids in gathering information about a person or organisation without their knowledge. On the Internet (where it is sometimes called a spybot or tracking software), spyware is



programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.

#### **SQL**

Structured Query Language (SQL) is a special-purpose programming language designed for managing data held in a relational database management system (RDBMS), or for stream processing in a relational data stream management system (RDSMS).

#### **SSD**

Like a memory stick, there are no moving parts to an Solid State Disk (SSD.) Rather, information is stored in microchips. Conversely, a hard disk drive uses a mechanical arm with a read/write head to move around and read information from the right location on a storage platter. This difference is what makes SSD so much faster.

#### **SSO**

Single sign-on (SSO) is a property of access control of multiple related, but independent software systems. With this property a user logs in with a single ID and password to gain access to a connected system or systems without using different usernames or passwords, or in some configurations seamlessly sign on at each system.

#### **Stateful Inspection**

Stateful packet inspection (SPI) is a firewall architecture that works at the network layer. Unlike static packet filtering, which examines a packet based on the information in its header, stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table.

#### **Switch**

In telecommunications, a switch is a network device that selects a path or circuit for sending a unit of data to its next destination. A switch may also include the function of the router, a device or program that can determine the route and specifically what adjacent network point the data should be sent to.

#### **TIPT**

Telstra Internet Protocol Telephony (TIPT) is a complete unified communications solution that's simple, flexible and scalable, and highly reliable. It allows you to converge voice, video and data on one network while providing a consistent user experience across devices and locations.

### **Trojan**

A Trojan is a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that it can get control and do its chosen form of damage, such as ruining the file allocation table on your hard disk.

### **UAT**

In software development, user acceptance testing (UAT) - also called beta testing, application testing, and end user testing - is a phase of software development in which the software is tested in the "real world" by the intended audience.

### **UPS**

An uninterruptible power supply (UPS) is a power supply that includes a battery to maintain power in the event of a power outage. Typically, a UPS keeps a computer running for several minutes after a power outage, gracefully shuts down the computer and powers it back on when the power is restored.

### **UTM**

Unified threat management (UTM) is a solution in the network security industry, and since 2004 it has become established as a primary network gateway defense solution for organizations. In theory, UTM is the evolution of the traditional firewall into an all-inclusive security product able to perform multiple security functions within one single system: network firewalling, network intrusion prevention (IPS), gateway antivirus (AV), gateway anti-spam, VPN, content filtering, load balancing, data loss prevention, and on-appliance reporting.

### **VCM**

VCM refers to a VMware vCentre Management server. A VMware vCenter Management server allows for the management of multiple ESX servers and virtual machines (VMs) from different ESX servers through a single console application.

### **Virtual Machine**

A virtual machine (VM) is a software implementation of a machine (i.e. a computer) that executes programs like a physical machine. Virtual machines are separated into two major categories, based on their use and degree of correspondence to any real machine. Multiple OS environments can co-exist on the same computer, in strong isolation from each other.

### **VoIP**

VoIP (voice over IP - that is, voice delivered using the Internet Protocol) is a term used in IP telephony for a set of facilities for managing the delivery of voice information using the Internet Protocol (IP). In general, this

means sending voice information in digital form in discrete packets rather than in the traditional circuit-committed protocols of the public switched telephone network (PSTN).

#### **VPN**

A VPN (virtual private network) is a way to use a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organisation's network.

#### **VSS**

Volume Shadow Copy (VSS) is a technology included in Microsoft Windows that allows taking manual or automatic backup copies or snapshots of computer files or volumes, even when they are in use.

#### **WAN**

A wide area network (WAN) is a geographically dispersed telecommunications network. The term distinguishes a broader telecommunication structure from a local area network.

#### **WAN Failover**

WAN failover allows the enabling of an interface as a secondary or backup WAN port. The secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through the secondary WAN port if the primary WAN port is down and/or unavailable.

#### **Wi-Fi**

A technology that allows electronic devices to connect to a wireless LAN (WLAN) network, mainly using the 2.4 gigahertz (12 cm) UHF and 5 gigahertz (6 cm) SHF ISM radio bands. A WLAN is usually password protected, but may be open, which allows any device within its range to access the resources of the WLAN network.

#### **WSUS**

Windows Server Update Services is a free add-on for managing patches and updates to the Microsoft Windows XP, Windows Server and Microsoft Office systems. Aimed mainly at small and medium-sized businesses WSUS is intermediate between the simpler Windows Update for individual computer users and the more robust Systems Management Server (SMS) for large enterprises.