FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

SHIRE OF COCOS KEELING ISLANDS
MAJU PULU KITA | ADVANCE OUR ISLANDS

Strategic I.T Plan 2022 - 2025

5, 443 Albany Hwy
Victoria Park, WA, 6100

p. 1300 664 136

Info@focus.com.au
www.focus.com.au

FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

Authorisation

This plan has been prepared by Focus Networks and is authorised by:

Frank Mills
Chief Executive Officer
Shire of Cocos Keeling Islands

FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

Document Control

Proposal for amendment or change to this document should be forwarded to:

Frank Mills
Chief Executive Officer
Shire of Cocos Keeling Islands
E-mail: frank.mills@cocos.wa.gov.au

Date	Version	Description of Changes	Author
01.08.22	0.1	Initial document creation	David Staeck
02.08.22	0.1	Initial meeting with Azia and Vikki	
10.08.22	0.2	Update Previous Goals/ICT Trends	David Staeck
11.08.22	0.3	Worked on the current state and future state sections for various items.	David Staeck Brad Parkes
21.09.22	0.3	We worked on the current state and future state sections for various items.	David Staeck Brad Parkes
10.10.22	0.3	Updated Appendix A Microsoft Licenses, Appendix C Computer Information,	Bradley Parkes
17.10.22	0.3	Worked on the current state and future state sections for various items.	David Staeck
28.10.22	0.4	Added budget information supplied by Azia	Bradley Parkes
11.11.22	0.5	Document review meeting and amendments	David Staeck
25.11.22	0.6	Draft client version released	David Staeck
25.01.23	1.0	The final client version released	Bradley Parkes Doug Cusens

FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

Distribution

The Chief Executive Officer controls the distribution of this plan.

Title	Name	Email Address
Chief Executive Officer	Frank Mills	frank.mills@cocos.wa.gov.au
Communications & IT Officer	Azia Bulka	comms@cocos.wa.gov.au
Operations Director (Focus Networks)	Doug Cusens	doug.cusens@focus.com.au

FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

Table of Contents

Executive Summary

Both the internal and external environments of The Shire of Cocos Keeling Islands (The Shire) are changing, and technology is a critical supporter of its services' development, implementation, and enhancement. This makes it imperative that there is an overall approach for the selection, use, and support of technology that aligns with The Shire's resources, business needs, and processes.

The Shire's Strategic Information Technology Plan (IT Plan) provides direction for addressing both short-term and long-term requirements for cost-effective, practical technological solutions. Through the investment in and use of advanced technology, The Shire can emphasise both external and internal customer services.

The Shire's plan provides a framework for effectively managing Information Technology (IT). The primary goal of IT is to support the business objectives of The Shire and to facilitate departmental efforts to provide efficient and effective services to its members, the public, and other stakeholders. The plan also provides a foundation for an enterprise-wide approach to the management of IT.

Many future technology efforts cross multiple departments with a single goal of providing services to its members, the public, and other stakeholders. This environment requires technology to be used as the basis for communication, interoperability, data, and resource sharing. Furthermore, technology is a vehicle through which cost reduction can occur by increasing the efficiency and effectiveness of services through corporate architecture and standards.

This plan is not intended to limit department autonomy but to provide a comprehensive roadmap focused on solving everyday problems and enabling collaboration. The plan is built on the IT management model, which utilises the best features of centralised IT management and outsourced IT support. The plan also requires developing IT architecture and standards, which are critical for actual economies of scale and interoperability.

The Shire's IT Plan provides a framework for effectively managing technology. It offers a customer-focused approach to implementing and managing technology from both an internal and external perspective. Internally it focuses on collaboration, shared input, and providing the right tools for its employees. Externally it focuses on delivering services expected by its members, the public, and other stakeholders.

As with all strategic plans, this plan is a "living document" that allows for changes over time and serves as a broad guideline for action. The nature of technological advances and changing The Shire's needs mandate plan revisions. The plan is designed to link The Shire's needs and goals with IT to provide improved functions and enhanced customer service. All technology decisions should be made strategically based on the initiatives outlined in this document. This ensures that all decisions can be made in an environment of flexibility but that the result achieves the goals and expectations set by The Shire.

Previous Goals and Achievements

The Shire has undertaken significant IT and business systems projects in recent years. These projects were conducted to streamline business processes, improve productivity and enhance system reliability.

Date	Project	Goal	Costs
June 2019	Server Replacement	Install the new Dell PowerEdge R640.	$28,000
January 2020	Office 365	Install and deploy desktop software.	$10,000
January 2020	Computer Refresh	Purchase HP laptops for Councillors.	$7,000
June 2020	TV for Council Chambers	Purchase Samsung TV and stand.	$2,500
December 2020	Computer Refresh	Purchase of Dell desktops/laptops.	$16,000
April 2021	Computer Refresh	Purchase of Dell desktops/laptops.	$20,000
Oct 2021	Video Conferencing	Installation of Logitech Meetup in Council Chambers.	$1,700
May 2022	Multi-Factor Authentication	Implementation of DUO MFA for Microsoft 365 and remote access.	$2,475
May 2022	UPS Replacement	Replacement at West Island Admin Building, Depot, and Home Island Admin Building.	$12,140
May 2022	Internet Comms	Installation of Business NBN satellite link on Home Island Admin Building.	$2,320
May 2022	Internet Gateway	Installation of SonicWall firewall on Home Island Admin Building.	$800
May 2022	Backup and Archive	Implemented Managed Recovery Service in Home Island Admin Building.	$2,530
May 2022	Computer Room	Cleaned up and made secure in Home Island Admin Building.	$3,990
May 2022	Local Area Network	Replaced switching and implemented RADIUS on Home Island Admin Building, Depot, and West Island Admin Building.	$11,970
May 2022	Restrict Admin Privileges	Implement named admin accounts, security groups, and group policies.	$3,630

*Pricing excludes GST

Emerging Trends and Technologies

This describes the emerging trends and technologies providing challenges and opportunities in managing ICT systems and resources and delivering future ICT services.

Trends and technologies in the IT industry change at an alarming rate. The Shire relies 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 corporations, as listed below from the ICT research and advisory firm - Gartner Inc.

Discussing these emerging trends should guide future decisions on Governance, Business Systems and Applications, Infrastructure and Technology, Business Continuity, Security, and Project Management.

ICT Trend	Explanation
Accelerated Legacy Modernisation	Governments have experienced the limitations and risks of decades-old legacy infrastructure and core systems. To be better equipped to deal with the next disruption, government CIOs are accelerating the move to modern, modular architectures. While the need for legacy modernisation is not new to government CIOs, the challenges related to the pandemic have only served to heighten the awareness of the resulting risks and the need for it. Gartner predicts that by 2025, over 50% of government agencies will have modernised critical core legacy applications to improve resilience and agility.
Adaptive Security	An adaptive security approach treats risk, trust, and security as a continuous and adaptive process that anticipates and mitigates constantly evolving cyberthreats. This approach features components for prediction, prevention, detection, and response. It forgoes traditional notions of the perimeter, assuming there is no boundary for safe and unsafe, a necessary conceptual shift given the migration to cloud services. Gartner predicts that 75% of government CIOs will be directly responsible for security outside of IT by 2025, including operational and mission-critical technology environments.
Anything-as-a-Service (XaaS)	XaaS is a cloud-only sourcing strategy that embraces acquiring the full range of business and IT services on a subscription basis. The pandemic response and the critical need for digital service delivery have exacerbated pressures to modernize legacy applications and infrastructure. XaaS offers an alternative to legacy infrastructure modernisation, provides scalability, and reduces the time to deliver digital services. Gartner predicts that 95% of new IT investments by government agencies will be as-a-Service solutions by 2025.
Case Management-as-a-Service (CMaaS)	Case work is the predominant workstyle of government, with the entire legacy-heavy portfolio of monolithic case management point solutions found in many departments. CMaaS is a new way to build institutional agility by applying composable business principles and practices, to replace legacy case management systems with modular products that can be rapidly assembled, disassembled, and recomposed in response to changing business needs.

ICT Trend	Explanation
	Gartner predicts that by 2024, government organisations with a composable case management application architecture will implement new features at least 80% faster than those without.
Citizen Digital Identity	Digital identity is the ability to prove an individual's identity via any government digital channel available to citizens, which is critical for inclusion and access to government services. Digital identity ecosystems quickly evolve and lead governments to assume new roles and responsibilities. The topic is high on political agendas, so government CIOs must link digital identity to salient use cases. Gartner predicts that a global, portable, decentralized identity standard will emerge in the market by 2024 to address business, personal, social, societal, and identity-invisible use cases.
Multichannel Citizen Engagement	Citizen direct participation with governments reached new heights in 2020 as communities dealt with the pandemic, wildfires, hurricanes, and other events. Multichannel citizen engagement is a seamless, bidirectional engagement with constituents across organisational boundaries while delivering a personalised experience using the preferred and most effective channels to reach them. Gartner predicts that over 30% of governments will use engagement metrics to track the quantity and quality of citizen participation in policy and budget decisions by 2024.

1. Governance

This describes the guiding strategies, principles, and practices that guide the correct and effective delivery of ICT and provides a framework for ICT decision-making. Elements to consider are as follows:

Element	Explanation
ICT Strategy and Planning	Conducting ICT strategic planning. Developing systems and delivering ICT services per an approved ICT Strategic Plan. Involving IT in corporate planning.
Risk Management	The identification, assessment, and prioritisation of risks. A coordinated and economical application of resources to minimise, monitor, and control unfortunate events' probability and impact.
ICT Procurement	Involves the acquisition of ICT goods and services.
Policy, Processes, and Procedures	Having documented and approved ICT policies, processes, and procedures that staff is aware of, have access to and are actively using.
Performance Measurement	The process for measuring and reporting the performance of ICT services is often measured through tools such as Key Performance Indicators (KPIs) or service level agreements.
Performance Management	These activities ensure that goals are consistently being met effectively and efficiently.
Monitoring and Compliance	Having measures and controls in place to monitor compliance with ICT controls, guidelines, and procedures. This includes audit logging of systems, identification of anomalies, and incident handling provisions.
ICT Resource Management	The efficient and effective use of ICT resources (information, systems, networks, infrastructure, devices, and people) to deliver ICT services.
ICT Sourcing Models	Alternative ways of delivering ICT services. Alternate ICT sourcing models include managed solutions provided by a service provider, shared services with another entity, and cloud computing.

1.1 IT Support Arrangements

1.1.1 Industry Best Practice

Outsourced IT services should include the following;

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

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

Organisations employing third-party IT support providers should regularly review the support schedule to ensure it meets business requirements.

1.1.2 Current State

The Shire has contracted Focus Networks to provide managed IT services. Support arrangements include;

- Scheduled onsite visits at least once a year.
- The ability to log urgent support requests 24x7x365.
- Proactive monitoring of the ICT network during business hours.
- Change management planning.
- Microsoft and third-party patch management.
- Monthly management reporting.
- Quarterly IT meetings.

The Shire has been granted access to the Focus Networks helpdesk portal and can review Helpdesk calls anytime. Scheduled onsite visits can be adjusted to suit seasonal shifts in IT support requirements or projects.

For the past three months, 94 IT support tickets were logged and resolved, equating to an average of 31 tickets per month.

The enterprise resource planning application (SynergySoft/Altus) is supported by IT Vision.

1.1.3 Future State Recommendations

The mix of IT providers and software vendors appears to be working well and meeting current needs. The various third-party support providers work together to provide strategy and direction for The Shire IT team, and communication is effective. All changes recommended in this category are non-essential and can be undertaken when requirements change.

1.1.4 Budget Estimate

The Focus Networks Managed Proactive Service is a managed service, which means all costs are monthly variable operational costs.

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Managed Proactive Service	$39,652	$40,842	$42,067	$43,329
TOTAL	$39,652	$40,842	$42,067	$43,329

*Pricing excludes GST and is a budget estimate only. Travel and accommodation costs once a year are included. Annual price increases predict 3% and are subject to change.

1.2 IT Risk Management

1.2.1 Industry Best Practice

Risk management seeks to identify, assess and prioritise risks within an organisation. Resources can then be economically coordinated to minimise, monitor, and control these risks' probability and impact. This risk management approach is equally well suited to managing IT risks within an organisation.

In smaller organisations, it is practical to document and manage IT risks following a similar methodology to other business risks. This will allow an existing Audit Committee or Risk Committee to review and action IT risks through existing mechanisms to maximize efficiency. This will ensure that IT risks are managed, and their associated risks are reduced over time.

Risk weighting is used to identify the consequences and likelihood of each risk before and after any controls are put into place. For example, the risk of computer malware can be easily identified with a high-risk rating relating to consequence and likelihood. However, controls such as anti-virus software and Internet gateway can significantly reduce the risks of these events.

1.2.2 Current State

The Shire was audited by Moore Australia for a combined finance audit/ General Computer Controls (GCC) audit in July 2022 and will be audited again in November 2022. As of May 2022, The Shire and Focus Networks started project work to improve IT Risk Management controls and practices.

The audit findings have been placed on the Shires Risk Register, and IT risks are better represented in the Shires Risk Register. IT Risks are risk-weighted, and controls are put in place to reduce associated risks to an acceptable level.

Significant additional controls are being implemented.

1.2.3 Future State Recommendations

An initial IT risk assessment, risk treatment methodology, and risk management strategy and plan should be included within existing risk management processes, which will seek to identify the following:

- IT assets (physical, software, information, and human).
- Respective threats for each asset.
- The consequence and likelihood of the threat.
- Existing controls.

The Audit Committee should regularly review the risks and their respective treatments to seek to improve and work to reduce risks continually. Ongoing audits from bodies such as the OAG and Moore Australia are to be expected, and an allowance to review and implement new controls regularly has been allowed for in the Budget Estimates table below.

1.2.4 Budget Estimates

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Project Implementation Service	$5,000	$5,150	$5,305	$5,464
TOTAL	$5,000	$5,150	$5,305	$5,464

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

2. Business Systems and Applications

This describes the software systems and applications used. Elements to consider are as follows:

Element	Explanation
Software Acquisition	The process of purchasing software, including software evaluation and defining user requirements.
Software Design and Development	The process of designing and developing software and applications.
Software Maintenance and Management	The process of maintaining, upgrading, supporting, and managing software systems and applications.
Business Process Analysis	Refers to the process of analysing and documenting the business processes.
Integration	Enabling the sharing of data between systems.
Requirements Definition	The process of identifying and documenting what the business needs are when acquiring or developing new software or modifying existing systems.
Software Scoping	Defining a software system's purpose, functions, and features.
Testing	Adequately testing software systems or upgrades before implementation, including test implementation and user acceptance testing.
Implementation	Describes the processes involved in getting new software operating properly in its environment, including installation, configuration, running, testing, training, and managing change.

2.1 Corporate Applications

2.1.1 Industry Best Practice

Due to corporate applications' varied nature, best practices are listed in this section. Application vendors typically release their best practice white papers for specific applications, and they 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, an FMS requiring a back-end database should utilise Microsoft SQL, and access to this data should be restricted as necessary. An alternative to an FMS is a document management system (DMS) such as Micro Focus Content Manager or SharePoint.

2.1.2 Current State

The Shire currently uses a flagship ERP system called SynergySoft provided from ITVision. More recently, The Shire has adopted the Altus Procurement module. However, due to Internet connectivity issues the Altus Payroll module was not implemented.

The Shire has integrated the SynergySoft suite, which has delivered a wide array of modules and features based around the everyday needs of council staff.

These products add significant efficiency and business value to The Shire's organisation. Synergysoft is coupled with a range of Business Process Management Services such as Payroll, Rates and Finance processing. This solution has been integral to conduct operations throughout the The Shire's work space.

The Shire has depended on SynergySoft for many years. Modules within the suite include Core Financials, Payroll, Purchase Ordering, Rates and Property, Receipting, and Workshop Management.

The InfoCouncil agenda management solution is tailored to the needs of Australian Local Governments and is heavily utilised by The Shire. Regular program updates are required as this product integrates closely with the Microsoft Office 365 platform.

2.1.3 Future State Recommendations

The SynergySoft ERP has been in use for many years and is transitioning into Altus modules. The acquisition of ITVision by ReadyTech will give The Shire access to the Open Office suite of products. ReadyTech also bought Open Office who are based in Melbourne. The Open Office suite is Microsoft centric meaning extracting data out and putting data in becomes easier. The Manager Finance and Corporate Services should undertake an assessment of future Altus modules and the Open Office suite as products like TechOne and Civica are simply too expensive.

The Shire should investigate options for an Advanced Business Intelligence reporting solution aimed to provide improved reporting of business activities across The Shire. The solution will provide reporting dashboards for each business unit. Three layers of reporting will be provided across Business Unit Manager / CEO / Councillors. Such a product to help could be Microsoft Power BI.

It is recommended that a learning management system (LMS) be investigated. A LMS is a software application or web-based technology used to plan, implement and assess specific learning processes.

The Manager Infrastructure will be investigating a Plant Management system which is free of charge through Main Roads.

2.1.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
SynergySoft Suite	$25,280	$26,038	$26,820	$27,624
CBA Point of Sales Solution	$708	$729	$751	$774
Councillor Collaboration SharePoint Site	-	$5,500	-	-
TOTAL	$25,988	$32,268	$27,571	$28,398

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3. Infrastructure and Technology

This describes the hardware and network infrastructure used to deliver ICT services. Elements to consider are as follows:

Element	Explanation
Infrastructure	Refers to the physical IT hardware such as servers, network equipment, and communications devices.
Architecture	Refers to the design of the infrastructure environment used to interconnect computers and users, including server room and network design.
Virtualization	Creating virtual (rather than actual) hardware platforms (server or desktop environment), operating systems, storage devices, or network resources.
Capacity Management	Managing IT resources to ensure resources such as disk space, memory, and processing capability meets current and future business requirements cost-effectively.
Communications and Network Management	The activities involved in managing a local and wide area network include data, voice, and internet communications.
Data Storage	The disk or network storage space, memory, or media required to store digital data.
IT Asset Management	To support strategic IT decision-making, the practice of effectively managing the life cycle of software and hardware assets, including acquisition, implementation, maintenance, utilisation, and disposal.
Systems Acquisition	The process of purchasing systems hardware and network equipment, including defining business requirements and system evaluation.
Systems Design and Development	The process of designing and developing hardware platforms, networks, and infrastructure architecture.

3.1 Antivirus

3.1.1 Industry Best Practice

An anti-virus solution should include the following features;

- Scheduled full system scans.
- Real-time scanning.
- Behavioural monitoring.
- 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 completed on all servers and client machines.

Real-time scanning can impact the performance of critical 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 critical systems.

Behavioural monitoring should also always be enabled to prevent the increasingly popular ransomware viruses that encrypt data. Suitable anti-virus applications can detect when software attempts to encrypt data and block that application before any significant damage occurs.

3.1.2 Current State

Trend Micro Endpoint Protection is installed on all laptops, desktops, and servers, representing approximately 30 devices.

This product includes the following features (and more):

- Scheduled full system scans.
- Real-time scanning.
- Behavioural monitoring.
- Anti-malware component(s).
- Centrally managed reporting.

These features have been configured and enabled for all machines requiring protection from viruses and malware.

Scheduled scans have been conducted a minimum of once per week and are completed on all computers and servers. These scans occur weekly at 12:30 PM on Friday for computers and weekly at 12:30 PM on Sunday for servers.

Behavioural monitoring is enabled to prevent the increasingly popular ransomware viruses that encrypt data. Trend Micro has already detected and prevented many outbreaks of ransomware viruses to date.

3.1.3 Future State Recommendations

The current state meets all requirements, although consideration of Endpoint Detection and Response (EDR) solutions should be considered for improved detection and response against breaches and incident responses.

The move to an EDR system should be considered for the next financial year to better protect against increasingly damaging ransomware attacks and Microsoft 365-related attacks. Such attacks would be very detrimental to an organisation.

3.1.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Hosted Anti-Virus	$1,536	$5,760	$5,933	$6,111
Hosted Anti-Spam	$2,496	$2,571	$2,648	$2,727
TOTAL	$4,032	$8,331	$8,581	$8,838

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.2 ISP Links

3.2.1 Industry Best Practice

Industry best practices dictate that most organisations' 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 should have the following characteristics:

- Provided by a Tier 1 or 2 ISP.
- Guaranteed bandwidth of at least 100Mbps (preferred 100Mbps or higher at the main office)
- 100Mbps (preferred 1Gb) for a cloud/hosted platform.
- Guaranteed contention ratio.
- Synchronous uplink.
- Corporate/Enterprise level SLA.

A different ISP than the primary connection should also provide a secondary Internet connection. The secondary link can be a slower specification service, as its primary function is to act as a backup connection when the direct 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 link to free up bandwidth from the primary link.

3.2.2 Current State

The following ISP links are currently active:

The Shire is currently utilising multiple satellite services. A business-grade Internet satellite service located on Home Island is an NBN solution. This Internet satellite service uses spot beam satellite architecture which means high capacity and extensive coverage for remote sites. Vocus Communications deliver this service.

A residential Internet satellite service on Home Island is also an NBN solution. This Internet satellite service is a low-capacity low coverage solution. IPSTAR delivers this service.

A residential Internet satellite service on West Island is also an NBN solution. This Internet satellite service is a low-capacity low coverage solution. IPSTAR delivers this service.

Site	Connection Type	Speed	Monthly Cost
Home Island	Vocus NBN Business Satellite	30Mbps/5Mbps	$850
Home Island	IPSTAR NBN Residential Satellite	25Mbps/5Mbps	$195
West Island	IPSTAR NBN Residential Satellite	25Mbps/5Mbps	$95

3.2.3 Future State Recommendations

The installation of the Vocus NBN business satellite on Home Island has increased the reliability and performance of several specific users.

The ideal outcome is for The Shire to gain access to the SUB.CO fibre optic cable that routes between Perth and Oman. The landing station is just off the coast of West Island and is currently being used by the federal government. Access to this cable is imperative as it will deliver business-grade access quickly. This reliable service will be expensive.

Access to fibre optics will allow The Shire to move more workloads into the cloud, adopt a new telephony solution and further improve disaster recovery abilities.

3.2.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Vocus NBN Business Satellite	$11,200	$10,506	$10,821	$11,146
IPSTAR NBN Residential Satellite	$2,340	$2,410	$2,483	$2,557
IPSTAR NBN Residential Satellite	$1,140	$1,174	$1,209	$1,246
SUB.CO Fibre	-	$13,000	$13,390	$13,792
TOTAL	$14,680	$27,090	$27,903	$28,740

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.3 Uninterruptable Power Supply

3.3.1 Industry Best Practice

Uninterruptable Power Supplies (or UPS) delivers online power quality and scalable battery runtimes for crucial 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 before host hardware and other equipment lose 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.

3.3.2 Current State

A project was recently undertaken to replace the aging administration server room UPS, which was out of warranty and had been suffering from battery failures. An Eaton 9PX 1500VA UPS with one Extended Battery Module was installed in the Home Island Admin Building computer room with an Eaton Environmental Monitoring Probe. This UPS is rated at 1500VA and powers the server cabinet.

This UPS will provide approximately 2 hours of uptime for the IT infrastructure in the event of a power outage. The virtual servers are configured to begin shutting down gracefully after around 20 minutes to ensure enough battery time remains for other connected systems.

Automatic shutdown procedures and parameters are configured in prolonged power outages or extreme temperatures/humidity. The parameters are currently 35 degrees Celsius and 90% humidity.

Other smaller Eaton 5P 850VA UPS units protect the smaller comms cabinets in the Home Island Admin Building (outside Vikki's office), at the Home Island Depot, and the West Island Admin Building.

3.3.3 Future State Recommendations

All UPS equipment currently meets the Shire's current requirements for five years. All UPS should have an up-time test completed every two years to ensure the uptimes indicated are accurate. This will confirm that the batteries are functioning correctly.

3.3.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Home Island Admin Building	$210	-	$216	-
Home Island Depot	$210	-	$216	-
West Island Admin Building	$210	-	$216	-
TOTAL	$630	-	$649	-

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.4 Desktops / Laptops

3.4.1 Industry Best Practice

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

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

A shift from small form factor desktop machines to "mini desktops" frees up office desk space for all staff. These machines are also more energy efficient and operate silently.

Business laptops ensure the availability of standard accessories and peripherals, including docking stations and extended batteries.

3.4.2 Current State

The Shire currently utilizes a mix of HP and Dell desktops and laptops in its fleet of ~30 computers. A manufacturer's three-year hardware warranty covers these machines, and the Shire works to replace devices based on a three-year life cycle. This previously equated to replacing all computers in one project.

In 2021 a computer replacement project was undertaken to replace out-of-warranty computers throughout the organisation. The replacement comprised of the following:

Dell OptiPlex desktops, Dell Latitude laptops.

A standard operating environment (SOE) of Windows 10 Professional and Microsoft Office 365 is used.

Windows updates are managed by Focus Networks utilising ConnectWise Automate. Remote control is available via ConnectWise Automate for IT support. Computers are connected directly to the wall ports for network connectivity, not through a telephony handset.

The Shire's computers include Office 365 applications as part of the SOE. A summary of current Microsoft 365 licenses is shown below. Please refer to Appendix A for a complete list of Microsoft licensing.

License Type	Quantity
Microsoft 365 Business Standard	7
Office 365 E1	3
Office 365 E3	32

3.4.3 Future State Recommendations

Focus Networks recommends undertaking work into upgrading the SOE operating system to Windows 10 feature release 22H2. A quick audit is required before January 2023 to remove unwanted Microsoft licenses and to move billing off Integrated ICT and onto Focus Networks.

The desktop and laptop fleet at The Shire has increased steadily over the years. Computer replacements should be staggered yearly to replace a third of the fleet yearly. Replacements help with cash flow and introduce cost savings and efficiencies over the long term. Replaced computers can be sent back to Focus Networks to be securely disposed of through the HD Destruction Service.

Focus Networks have seen hardware leasing become much more widespread and cost-efficient than outright purchasing. A hardware leasing model should be compared against outright purchasing during the next refresh.

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

Description	Current Replacement Costs
Dell Optiplex desktop (accessories and screens)	$2,600
Dell Latitude laptop (accessories and screens)	$3,200

3.4.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Dell Optiplex Desktop Replacement	$5,200	$13,000	$13,000	$2,600
Dell Latitude Laptop Replacement	$12,800	$25,600	$3,200	$9,600
Microsoft 365 E3	$12,180	$12,545	$12,922	$13,309
Microsoft 365 Business Standard	$1,428	$1,471	$1,515	$1,560
Secure Disposal of Computers	$927	$955	$983	$1,013
TOTAL	$32,535	$53,571	$31,620	$28,083

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.5 Servers

3.5.1 Industry Best Practice

Physical server hardware should be specified that supports a virtual server environment. Virtual server environments provide the best possible return on investment due to increased server hardware utilization. If uptime is essential, the N+1 architecture delivers a minimum of two physical servers that use a software-defined storage solution.

The IT Industry has observed a significant shift to virtual server environments, which started a decade ago in the enterprise market space. This trend has recently migrated to the small-to-medium business market as vendors target their pricing and products towards the price-sensitive end of the market.

Current offerings of server hardware provide more performance which can be employed to support multiple servers on one server. This approach makes the best use of expensive server hardware. Virtual servers allow effective management of shared server storage and can be leveraged to reduce downtime.

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

- Redundant power supplies.
- Redundant cooling.
- Redundant 10GB network connectivity.
- Redundant hard drive configurations (RAID5 + hot spare disks).

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

3.5.2 Current State

A server replacement project was undertaken in June 2019 to place a Dell Power Edge R640 server onsite in the Home Island Admin Building computer room.

A new server provided current-generation solid-state server hard drives and significantly faster 1 Gbps networking connectivity. Options to provide additional server hardware for redundancy were not adopted at this stage.

The Dell server warranty expires in June 2024, when the server infrastructure will be five years old. Consideration of a hybrid cloud migration before June 2024 should be investigated if Internet access is available using the SUB.CO fibre.

The Dell PowerEdge R640 physical rack-mounted server uses the free Microsoft Hyper-V virtualization platform.

The Dell PowerEdge R640 physical server is configured with the following:

- 2 x Intel(R) Xeon(R) Silver 4215 CPU @ 2.50GHz.
- 2 x 800GB SSD hard drives, 6 x 600GB SAS hard drives.
- 96 GB RAM.
- Dual 900W power supplies.
- 2 of 4 network ports are used on 1Gbps NIC.

Microsoft Server licenses have a renewal via an annual CSP licensing. Annual CSP licenses ensure an annual review is undertaken to cover the Shires licensing obligations and provide access to the latest Server Operating System versions via Microsoft Software Assurance. Five virtual servers are running within the Microsoft Hyper-V virtual environment being:

Hostname	Description and Roles
COC1-PMW-DC01	Windows Server 2019 Standard Primary Domain Controller DNS DHCP
COC1-PMW-HV01	Windows Server 2019 Standard Hypervisor
COC1-PMW-MGMT01	Windows Server 2019 Standard Unifi CA NPS
COC1-PRW-RD01	Windows Server 2019 Standard File/Print Remote Desktop Services SynergySoft
COC1-PWW-WEB01	Windows Server 2019 Standard Altus Web Proxy IT Vision Universe

3.5.3 Future State Recommendations

As the server has recently been replaced and an end-of-life date is documented, the future requirements revolve around investigating a hybrid cloud option.

Discussions are required in March 2023 to setup a budget for the 23-24 financial year. The Shire has time to consider an approach to cloud services being a private cloud, a hybrid cloud, or the continuation of on-premise infrastructure. Without confirmation that access will be granted to business-grade Internet via the SUB.CO fibre, we can only assume that this access will be forthcoming.

3.5.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Segregate Network	$990	-	-	-
Patch Physical Server	$660	-	-	-
Microsoft Server CSP Licenses - RDP	$1,425	$1,468	$1,512	$1,557
Microsoft Server CSP Licenses – Std Server	$1,383	$1,424	$1,467	$1,511
Microsoft Server CSP Licenses – User CALs	$540	$556	$573	$590
HPE MicroServer Installation	-	$6,100	-	-
Private Cloud – DC01	-	$5,680	$4,141	$4,265
Private Cloud – MGMT01	-	$5,080	$3,523	$3,628
Private Cloud – RD01	-	$8,080	$6,613	$6,811
Private Cloud – WEB01	-	$4,780	$3,214	$3,310
TOTAL	$4,998	$33,168	$21,041	$21,673

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.6 IP Telephony

3.6.1 Industry Best Practice

IP Telephony is the technology that allows telephone conversations over the Internet or a dedicated IP network (instead of dedicated voice transmission lines).

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

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

Client computers should be connected to the local area network (LAN) via the associated VOIP phone handset; therefore, all VOIP phone handsets should allow gigabit connectivity to the network. Connecting client computers to the LAN through VOIP headsets does reduce switching and cabling costs.

3.6.2 Current State

The Shire currently utilise an Avaya IP500 V2 physical appliance located in the Home Island Admin Building outside Vikki's office. The Depot also uses this system through a network connection. No support contract exists for this system, but CCIT has offered assistance.

The West Island Admin Building uses a Uniden DECT cordless handset.

The Home Island phone system uses the number range:

- 089162 6649

The West Island phone system uses the number range:

- 089162 6740

The Avaya IP500 V2 has approximately 20 handsets. Currently, all calls are routed in and out through the IOTT satellite network.

3.6.3 Future State Recommendations

As the physical Avaya IP500 V2 physical appliance is currently out of support and represents a single point of failure, it is advised that The Shire explore moving to a more resilient phone system with advanced telephony features and PBX capabilities.

Microsoft Teams calling is a cloud-delivered service that provides many of the same functions as premises-based unified communications (UC) solutions. For this to work effectively, reliable Internet connectivity is always required as access to the SUB.CO fibre has not been determined; it is safer to commit to a telephony solution that sits on-premise instead of in the cloud.

A workable solution would be the Sangoma platform that sits on-premise on Home Island as a virtual appliance or a hardware device. Key staff on Home Island, West Island, and the Depot could use physical handsets. All other users would use a softphone that runs off their desktop or laptop as software. The advantage of this solution is that it relies less on a stable Internet connection.

3.6.4 Budget Estimate

A hosted on-premise IP Telephony or private cloud virtual PBX could be deployed via an OpEx model to reduce up-front expenditure. This is essentially a cost-per-handset model. The forward financial plan would need to be updated with future upgrades to the phone system.

A Sangoma virtual appliance or hardware device hosted on-premise on Home Island would be deployed. The license itself and physical handsets are an upfront purchase. After the first year, annual licenses and support renewals are required.

A Konftel video conferencing solution that integrates with the Sangoma telephony solution will deliver an integrated video conferencing solution for the Council Chambers.

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Sangoma SMB Download	-	$1,500	-	-
Titanium Support	-	$3,900	$975	$975
Sangoma P320 Handset	-	$3,500	-	-
Managed Telephony Service	-	$1,200	$1,200	$1,200
Ordering, Setup, Training Labour	-	$5,775	-	-
Konftel Council Chambers VC	-	$3,000	-	-
SIP Service	-	$3,000	$3,090	$3,183
TOTAL	-	$21,875	$5,265	$5,358

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

3.7 Printing

3.7.1 Industry Best Practice

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

Where required, additional printers can be deployed. However, these should always be laser printers sourced from a Tier 1 vendor 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. Secure Print allows for secure and confidential printing in a centralized printing environment.

3.7.2 Current State

Centralized printing has been implemented using a mixture of Kyocera TASKalfa 4052ci KX's, Kyocera M2040dn, and Ricoh SP 3610SF. Printer deployment is automated via group policy. Several smaller Dell printers are also in operation via USB. Secure Print has not been implemented.

3.7.3 Future State Recommendations

Replacement printers are considered in the forward capital replacement program. A lease vs. purchase consideration can be made at the time, including managed printing costs.

A large-format multi-function printer should be considered to facilitate printing that matches the business use case with specifications such as paper capacity, printing resolution, connectivity, and supported paper size. Ideally, a multi-function printer that securely releases personal print jobs across multiple devices.

The current RICOH SP multi-function printer was purchased in June 2019 and is also planned for replacement.

3.7.4 Budget Estimates

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Replacement Printers	-	-	$20,000	$20,000
TOTAL	-	-	$20,000	$20,000

*Pricing excludes GST and is a budget estimate only. Annual price increases are predicted and subject to change.

4. Business Continuity

Business Continuity describes the activities undertaken to enable and perform critical functions and deliver ICT services. Elements to consider are as follows:

Element	Explanation
Disaster Recovery	Involves all activities required to restore a system, service, or data to its state before a disaster or the closest achievable state depending on the success of the disaster recovery operation.
Contingency Planning	Refers to planning for alternative business outcomes to mitigate against risk.
Backups	Backing up data and systems and storing them offsite to ensure that data and systems can be recovered as required.
Replication	Involves replicating data and systems to a secondary site to provide resiliency and business continuity in case of an unplanned event or disaster.
Redundancy	Options for systems, networks, and communications links to mitigate risk and provide resiliency and business continuity.
Data Recovery	The process involved restoring data following an unplanned event or disaster.

4.1 Backups and Disaster Recovery

4.1.1 Industry Best Practice

Gartner, IDC, Forrester, and Yankee Group report that, on average, IT system downtime costs between $84,000 and $108,000 per hour. Additionally, it is reported that 90% of businesses that lose all their data go out of business within the following 12 months. Corporate data protection is achieved through a complete backup and replication solution consisting of 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 under the organization's recovery point objective (RPO). Ideally, incremental backups for an organization with normal 8 AM - 6 PM operating hours should occur every hour if suitable. Incremental backups 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 six months of backups stored. This device is also responsible for replicating 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 of a 10km 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.

4.1.2 Current State

The Shire outsources the backup and recovery tasks to Focus Networks via the Managed Recovery Service. The currently employed system consists of the following;

Onsite Server Backups
The onsite backups are stored on the supplied onsite MRS server, which resides in the Admin Building computer room. Military-grade AES 256-bit encryption is utilised, and this process will occur at least once an hour.

Server Name	Backup Technology	Job Details
COC1-PMW-DC01 COC1-PW-MGMT01 COC1-RMW-RD01 COC1-PWW-WEB01	Veeam	Managed by Focus Networks Onto separate server storage onsite Runs hourly Includes VSS snapshot (complete virtual machine) Daily notifications checked by Focus Networks

Offsite Server Backups
The backups maintained on the supplied onsite MRS server will be replicated onto an offsite MRS server which resides in the NextDC data centre in Western Australia. Military-grade AES 256-bit encryption is utilised, and this process will occur at least once per day.

Server Name	Backup Technology	Job Details
COC1-PMW-DC01 COC1-PW-MGMT01 COC1-RMW-RD01 COC1-PWW-WEB01	Veeam	Managed by Focus Networks Onto separate server storage offsite in NextDC in WA Runs daily Includes VSS snapshot (complete virtual machine) Daily notifications checked by Focus Networks

Public Cloud Backups
The Microsoft 365 platform has backups replicated onto an offsite MRS server which resides in the NextDC data centre in Western Australia. Military-grade AES 256-bit encryption is utilised, which will occur at least every four hours.

Platform	Backup Technology	Job Details
Business OneDrive Exchange Online Teams SharePoint Online	Veeam	Managed by Focus Networks Onto separate server storage offsite in NextDC in WA Runs every four hours Daily notifications checked by Focus Networks

Retention Period
The backups maintained on the Focus Networks supplied onsite MRS server, and the Focus Networks offsite MRS server are defined below:

	Number Kept Onsite	Number Kept Offsite	Explanation
Hourly	210	-	Hourly backups for two weeks.
Daily	-	31	Daily backups for one month.
Weekly	-	8	Weekly backups for two months.
Monthly	-	6	Monthly backups for six months.
Biannual	-	14	Biannual archive for seven years.

This backup and recovery solution allows the ability to restore data at the file level at any time. It provides a service level agreement highlighting the solution's recovery time objective and recovery point objective, with Primary or Secondary sign-off.

This backup and recovery solution includes a full annual Disaster Recovery test and a monthly verification test to ensure the systems operate as intended. The Disaster Recovery test is held at the Focus Networks office at no extra cost to The Shire. A Disaster Recovery test must be completed before December 2023 to document a successful outcome.

4.1.3 Future State Recommendations

Although the current state meets many requirements, The Shire acknowledges several opportunities exist to improve current systems.

A possible increase in Internet bandwidth by using the SUB. Co-fiber will result in the daily offsite backup being completed more than once daily. Another suggestion relating to the OAG is for The Shire to complete a file and folder restoration exercise every three months. Focus Networks can manage this process. A total disaster recovery test is conducted annually.

4.1.4 Budget Estimate

See the following table for an indication of on-going costings. For budget purposes, the data on-premise component is set to grow by 15% per annum.

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Managed Recovery Service On-Premise	$5,520	$5,686	$5,856	$6,032
Managed Recovery Service Public Cloud	$2,736	$2,818	$2,903	$2,990
File/Folder Restoration	$1,320	$1,360	$1,400	$1,442
TOTAL	$9,576	$9,863	$10,159	$10,464

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

4.2 IT Disaster Recovery Plan

4.2.1 Industry Best Practice

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

The IT DR Plan must also:

- Provide the information and procedures necessary to:
  - Respond to an occurrence.
  - Notify personnel.
  - Assemble recovery teams.
  - Recover data.
  - Resume processing at the current or alternate site as soon as possible after a disaster has been declared.
- Create a disaster recovery structure strong enough to guide all interrelated groups yet flexible enough to allow staff and teams to respond to whatever disaster may occur.
- Identify those activities necessary to resume complete services at the reconstructed disaster site or new permanent facility.
- Establish a return to a "business as usual" environment.

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

4.2.2 Current State

The Shire has not completed a Business Impact Analysis exercise and does not have a comprehensive IT DR Plan. Since 2020 new systems and technologies have been implemented at the Shire. These have not been reviewed to confirm how they may affect the restoration of IT systems in the event of a disaster.

Currently, there are no defined MTO, RTO, and RPO figures and no structure to assess, record, or communicate a disaster recovery situation.

4.2.3 Future State Recommendations

The Shire's IT DR Plan should be created based on the findings of the Business Impact Analysis exercise. The Managed Recovery Service needs to be referenced to align with the MTO, RTO, and RPO figures.

The IT DR Plan should be reviewed annually in subsequent years or with significant business changes. A review of core business applications and recovery objectives is required.

4.2.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
IT Disaster Recovery Plan	$5,670	$1,700	$1,751	$1,804
TOTAL	$5,670	$1,700	$1,751	$1,804

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

5. Security

Security protects information and systems from unauthorized access, use, modification, disclosure, or destruction. Elements to consider are as follows:

Element	Explanation
Access Management	Involves the management of user access to systems, including assigning and revoking privileges and permissions, authentication, and authorisation procedures.
Authentication	The process by which users are identified on a system or network.
Audit	Examining the management controls within IT infrastructure to determine if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve goals or objectives.
Remote Access	Providing access to information systems for staff working outside the local area or wide area network.
Incident Management, Reporting, and Response	Involves identifying, analysing, reporting, and responding to IT security incidents, including taking corrective and preventative action.
Physical and Environmental Security	Refers to providing adequate physical and environmental protection of ICT assets to prevent unauthorized access, use, or destruction.
Network and Communications Security	Taking measures to secure local and wide area networks, voice communications, and internet links.
Change Management	The process for directing and controlling alterations to the information processing environment. Change Management includes alterations to desktop computers, the network, servers, and software but typically refers to changes in processes and workflows that can become disruptive if not managed properly.
Version Control	The process of managing multiple versions of software and electronic files.

5.1 Domain

5.1.1 Industry Best Practice

Microsoft Active Directory (AD) is key to the centralized management of ICT networks. Active Directory has four primary functions.

- Authentication.
- Policy-based Administration.
- Security Policies for User Accounts.
- 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 utilizes authentication for login or access should be integrated with the domain to use domain authentication. AD Authentication reduces the number of credentials a user must remember, allowing a "Single Sign-on" (SSO) environment.

Microsoft Group Policy allows ICT administrators to standardize 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 implemented using Group Policy.

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

- Password policies.
- Account lockout policies.
- Account expiry policies.

Active Directory should be utilized to publish connection information about shared resources. For example, printer resources might be published in a domain to facilitate user searches.

5.1.2 Current State

Active Directory is present, well-structured, and up-to-date. The domain is utilising security groups to handle NTFS permissions.

Group Policy is being utilised for network drive mapping, printer mapping, software installation, and lockdown of public computers.

A detailed naming structure for IT equipment exists and allows administrators to see who owns the equipment, which suburb it is in, what office it is in, and what kind of equipment it is. An example is SCKCKIAWKS1. The "SCK" indicates that the item belongs to The Shire domain. The "CKI" means the item belongs to the Cocos Keeling Islands locality. The "A" indicates the device is in the head office. "WKS" indicates the device is a workstation.

The Shire meets current state requirements as no new forest or domain functional levels have been added since Windows Server 2016. Later operating system versions can and should be used for domain controllers. However, Cocos Keeling Islands uses Windows Server 2016 as the most current functional level. The domain also has DFS-R as the engine to replicate SYSVOL.FSMO (Flexible Single-Master Operations) roles used by Active Directory.

DHCP is automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

5.1.3 Future State Recommendations

Focus Networks recommends the following;

- Usage of access-based enumeration for file shares.
- The intent is to limit the network drive mappings as much as possible. Limiting network drive mapping will also enable greater control and auditing of access to corporate data.
- Review of group policies to ensure Windows 10 and later versions of office are correctly handled
- Review the Password Policy to move from a traditional password to a passphrase. The benefit for users is to reduce the password change frequency to a year or more.

5.1.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Top Level Domain Project	$990	-	-	-
Complete NTFS Audit	$1,980	-	-	-
Admin User Audit	$990	-	-	-
Onboarding/Offboarding Procedure	$990	-	-	-
Implement Name Based Accounts	$2,475	-	-	-
Implement Date of Birth Security	$330	-	-	-
Implement Azure AD	-	$1,980	-	-
Review Existing Group Policies	-	$990	-	-
Implement Password Policy	-	$660	-	-
TOTAL	$7,755	$3,630	-	-

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

5.2 Internet Gateway

5.2.1 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:

- Gateway Antivirus.
- Gateway Antispyware.
- Intrusion Prevention.
- Application Intelligence and Control.
- Web/Content Filtering.
- 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 provide granular control and real-time visualization of applications to guarantee bandwidth prioritization to ensure maximum network security and productivity.

5.2.2 Current State

Two managed SonicWall firewalls exist at the Home Island Admin Building and West Island Admin Building. The firewalls have extensive reporting and deep packet inspection (DPI). A replacement contract covers firewalls, and regular firewall auditing is carried out.

Site	Firewall Model	Security Services
Home Island Admin Building	TZ270	GAV/GAS/IPS/CFS
West Island Admin Building	TZ270	GAV/GAS/IPS/CFS

The Home Island Admin Building firewall terminates a 30/5Mbps Vocus Business satellite service and a 25/5Mbps IPSTAR NBN residential satellite service. A current project is underway to implement a firewall in the West Island Admin Building to terminate a 25/5Mbps IPSTAR NBN residential satellite service.

A UPS powers all firewalls for protection and improved uptime.

The SonicWall SSL VPN service provides remote access to the network configured on the Home Island Admin Building. DUO MFA protects the SonicWall SSL VPN. Limited RDP use is supplied for ITVision, secured to several static internet addresses for improved security.

5.2.3 Future State Recommendations

The SonicWall firewalls will need to be upgraded in the 25/26 financial year. Upgrades due to Internet links becoming faster or the request to enable more security services. Both firewalls require more processing power, so the SonicWall firewalls are swapped out for a more significant device at a higher monthly cost.

5.2.4 Budget Estimate

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

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Home Island Admin Building	$1,620	$1,669	$1,719	$2,640
SSL VPN 5 Pack	$180	$185	$191	$197
West Island Admin Building	$2,040	$2,101	$2,164	$2,640
TOTAL	$3,840	$3,955	$4,074	$5,477

* Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

5.3 Computer Room

5.3.1 Industry Best Practice

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

- Independent and redundant air-conditioning.
- Backup ventilation fan.
- Dedicated 15A+ (or higher) power circuit for each UPS.
- Sufficient storage for IT hardware, extra cabling, and software.
- Non-carpet flooring to minimize dust.
- Lockable door.

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

5.3.2 Current State

The Home Island Admin Building has a multi-purpose room used as a computer room. It houses a lockable half-height server rack containing a firewall, switches, server, UPS, and internet connections.

The split air conditioner is the first line of defence in maintaining the stability of the computer room. The reliability of cool air is directly related to the server's uptime.

Physical security is lacking because any staff can access this multi-purpose room. This multi-purpose room's door is flimsy and cannot be locked.

The Home Island Depot has an office upstairs. The office houses a lockable wall-mounted communications rack containing switches and a UPS. The split air conditioner maintains cool air, but the equipment located in the wall-mounted communications rack requires minimal cooling. Physical security is increased as the office can be locked.

The West Island Admin Building has a ground-floor office close to the airport. The West Island Admin Building houses a lockable wall-mounted communications rack containing a firewall, multiple switches, and a UPS. The split air conditioner maintains cool air, but the equipment located in the wall-mounted comms rack requires minimal cooling. Physical security is increased as the office can be locked.

A project is currently in progress to install a wall-mounted communications rack outside Vikki's office. The project will include terminating network cables, placing two switches, and a UPS in the wall-mounted communications rack. This lockable wall-mounted communications rack will increase physical security. The existing telephony system on the wall will be removed next year.

5.3.3 Future State Recommendations

Focus Networks advises that all keys to server racks or wall-mounted communications cabinets be physically removed, labelled, documented in a key register, and stored in a safe place.

A small project must be completed to install a solid door for the Home Island Admin Building computer room. The door should be lockable from the outside, and its key labelled, documented in a key register and stored in a secure, safe place. The door should be locked and access restricted.

To bolster security further, a small discrete CCTV camera could be mounted inside the Home Island Admin Building computer room. A CCTV camera should be positioned to view the server rack, but staff must be aware that it is recording.

The destruction of old IT equipment is essential. It was noted that old IT equipment is stored in the storage room adjacent to the Home Island Admin Building computer room. We do understand that moving equipment off the islands is expensive. If equipment is moved off the islands, it must be "electronically destroyed" before moving off them. Physical destruction ensures that components are rendered useless.

It is also suggested to install a smoke alarm in the Home Island Admin Building computer room. This device should be inspected annually.

5.3.4 Budget Estimate

See the following table for an indication of ongoing costings:

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Home Island Admin Building – Comp Room Door	$1,000	-	-	-
Home Island Admin Building – CCTV	$1,000	-	-	-
Home Island Admin Building – Smoke Alarm	$500	-	-	-
West Island 18RU Wall Mounted Cabinet	$1,000			
TOTAL	$3,500	-	-	-

* Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

5.4 Local Area Network

5.4.1 Industry Best Practice

Core network switching should provide the following;

- Layer 3 routing functionality.
- Management interface.
- Power over Ethernet.
- At least 1000Mbps (1 gigabit) connectivity to all computers.
- At least 10000Mbps (10 gigabits) connectivity to all servers.

Additionally, core network switching should permanently be configured in a redundant stack.
Local area networks should utilize VLAN encapsulation for logical segregation of network traffic.

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 to increase security using SSIDs, VLANs, and user authentication.

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

5.4.2 Current State

Focus Networks refreshed the switching infrastructure in May 2022. The refreshment involved implementing managed Ubiquiti Edgeswitch devices. Faster access to the physical server with network redundancy was implemented.

Due to time constraints, the 802.1X Port-based Network Access Control (PNAC) authentication via RADIUS was partially setup.

Site	Network Switches	Date of Purchase
Home Island Admin Building Comp Room	Ubiquiti EdgeSwitch ES-24-250W 24 Port Gigabit	May 2022
Home Island Admin Building Comp Room	Ubiquiti EdgeSwitch ES-24-250W 24 Port Gigabit	May 2022
Home Island Depot	Ubiquiti EdgeSwitch ES-24-250W 24 Port Gigabit	May 2022
Home Island Depot	Ubiquiti EdgeSwitch 16-150W 16 Port Gigabit	Unknown
West Island Admin Building	Ubiquiti EdgeSwitch ES-24-250W 24 Port Gigabit	May 2022
West Island Admin Building	Ubiquiti EdgeSwitch ES-24-250W 24 Port Gigabit	May 2022

The previous IT provider installed a series of Ubiquiti wireless access points. These Ubiquiti wireless access points provide corporate WIFI and Visitors WIFI. Due to time constraints, the Extensible Authentication Protocol (EAP) was partially set up. A current project is underway to move the two existing Ubiquiti wireless access points from the Home Island Admin Building into the Home Island Depot. Two new Ubiquiti wireless access points will be installed in the Home Island Admin Building in January 2023.

A current project is underway to implement outdoor point to point wireless (P2P) between the Home Island Depot and the Home Island Admin Building. This project involves using the Azmie Zaitu building as a connection or junction point. A spare wireless access point sits in the Home Island Admin Building with Azia. This work is to move The Shire off the IOTT network.

A current project is underway to implement a site to site VPN tunnel between the West Island Admin Building and the Home Island Admin Building. This will utlise a firewall and the NBN satellite links at each end. This work is to move The Shire off the IOTT network.

Site	Wireless Access Points	Purchase Date
Home Island Admin Building - Chambers	1 x Ubiquiti U6-Pro	Jan 2023
Home Island Admin Building – Office	1 x Ubiquiti U6-Pro	Jan 2023
Home Island Depot	2 x Ubiquiti AC-Lite	Unknown
West Island Admin Building	1 x Ubiquiti AP-Pro	Unknown
Home Island Admin Building	1 x Ubiquiti Nanobeam G2 airMAX	Jan 2023
Home Island Depot	1 x Ubiquiti Nanobeam G2 airMAX	Jan 2023
Home Island Azmie Zaitu	2 x Ubiquiti Nanobeam G2 airMAX	Jan 2023

5.4.3 Future State Recommendations

Minimal future work is required for security on the local area network. The outstanding implementation of the 802.1X Port-based Network Access Control (PNAC) authentication via RADIUS on the switches needs completing. The outstanding implementation of the Extensible Authentication Protocol (EAP) on the wireless network needs to be completed.

Maintenance on the outdoor point to point wireless will be required. This involves physically sighting the installations to make sure the weather conditions have not moved the equipment which affects alignment and performance.

A current project is underway to implement outdoor point to point wireless (P2P) between the Home Island Parks Office and the Home Island Admin Building. This project involves using the Community Shelter building as a connection or junction point. This work is to move The Shire off the IOTT network.

Of most importance is to implement a point to point wireless link between West Island and Home Island. This involves a licensed spectrum link using the 11GHz band. A 5 nautical mile link over water presents challenges. This link has to be installed by professionals on towers at high heights and checked every two years. This will complete the task of moving off the IOTT networks.

5.4.4 Budget Estimate

See the following table for an indication of ongoing costings:

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Home Island Admin Building - Chambers	$750			
Home Island Admin Building – Office	$750			
Home Island Admin Building – P2P	$1,250		$340	
Home Island Depot – P2P	$1000		$340	
Home Island Azmie Zaitu – P2P	$1,250		$340	
Home Island Depot	$500		$340	
Home Island Community Shelter – P2P	$1,500		$340	
Home Island Parks Office – P2P	$1,250		$340	
West Island to Home Island – P2P		$42,000		$5,000
TOTAL	$8,250	$42,000	$2,040	$5,000

*Pricing excludes GST and is a budget estimate only. Annual price increases predict 3% and are subject to change.

5.5 Patching

5.5.1 Industry Best Practice

Patching keeps systems and applications running smoothly but is also the core activity keeping your organization secure.

Effective patch management includes:

- Discovery – have a comprehensive network inventory.
- Categorize – split this into servers, computers, and network devices.
- Monitor – keep an eye on different vendor release dates.
- Testing – create test groups where possible.
- Change Management – have a rollback plan in case issues occur.
- Reporting – gain more visibility through compliance reports.

Patching can be time-consuming, so these tasks should be automated wherever possible. Applying patches under specific conditions is ideal. There will be some instances where manual intervention is required.

For most environments, servers and computers should be patched monthly after the Microsoft patch Tuesday, following a suitable regime for the organization. Of importance is the Windows 10 operating system, which has multiple versions released every year. A version number, codename, build number, and release date must be understood as support ends for older versions.

For most environments, servers and computers should also be patched monthly for third-party software. This can be referred to as third-party application patching and covers applications like Adobe, Java, and Chrome.

A scheduled maintenance program should ensure that firmware updates are applied to networked devices such as:

- Internet Gateways.
- Routers.
- Network Switches.
- Wireless Access Points.
- Physical Servers.
- Network Printers.
- Phone Systems.

Finally, it is recommended to undertake scheduled vulnerability scans of the corporate network to ensure no underlying vulnerabilities are still in place that could expose the corporate network to viruses or other cyber incidents. Vulnerability scanning is a way to ensure that all patching and remediation works are working effectively.

5.5.2 Current State

Windows updates are configured and installed weekly by the ConnectWise Manage agent on each computer. A defined test group for computers is established, meaning these computers receive Windows updates before all other computers. This is to ensure that Windows updates do not have undesired consequences.

Windows 10 feature releases for Windows 10 computers require manual installation. We use tools to do a silent install on the user's computer, which completes the installation after reboots.

Windows updates are configured and installed monthly by the ConnectWise Manage agent on each server. Servers do not have a defined test group, meaning they receive Windows updates. Depending on the size and nature of the Windows update, the server can be manually backed up before the Windows update is applied.

Third-party patching is configured and installed weekly by the ConnectWise Manage agent on each computer. There are no defined test groups for computers. Typical third-party applications include Adobe, Chrome, iTunes, and Zoom.

The scheduled maintenance program to update the firmware on networked devices is completed once a year. Scheduled maintenance is conducted over the XMAS and New Year break. Scheduled outages occur when the business is shut down.

5.5.3 Future State Recommendations

The scheduled maintenance program to update firmware on networked devices should be completed more regularly. A move to twice a year and up to four times a year should be investigated.

If referencing the ASD Essential 8 or the OAG, internal vulnerability scans are required to assist in detecting and resolving security issues. The Nessus Pro tool should be scheduled and completed every quarter to highlight security issues. Remediation works then proceed. This tool gives an excellent overview of the current patching systems' effectiveness.

If referencing the ASD Essential 8 or the OAG, external vulnerability scans are required to assist in detecting and resolving security issues. The Tenable.IO tool should be scheduled and completed monthly to highlight security issues on external facing web applications and portals. Remediation works then proceed. This tool gives an excellent overview of application vulnerabilities.

5.5.4 Budget Estimates

See the following table for an indication of ongoing costings:

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Maintenance Program	$1,260	$1,298	$1,337	$1,377
Internal Vulnerability Scans	$4,800	$4,944	$5,092	$5,245
External Vulnerability Scans	$2,120	$2,184	$2,249	$2,317
TOTAL	$8,180	$8,425	$8,678	$8,939

*Pricing excludes GST and is a budget estimate only. Annual price increases are predicted and subject to change.

5.6 Cyber Response

5.6.1 Industry Best Practice

Strategies to mitigate cyber security incidents are listed at cyber.gov.au and are referred to as the Essential Eight. They are listed as:

- Prevent malware delivery and execution.
- Limit the extent of cyber security incidents.
- Recover data and systems availability.

A cyber incident response plan can then be created. Such a plan has a similar layout to an IT DR plan. There is an Introduction, Terminology and Definitions, Common Cyber Incidents and Responses, Roles and Responsibilities, and an Incident Response Process. A cyber incident response plan protects your data, reputation, and revenue.

Security awareness training is recommended for employees who complete authorized functions online for their employer. Necessary knowledge will help to defend themselves and secure their employer's assets from damage or loss. Training can be broken up into three elements:

- Programs to train employees to protect against cyber threats.
- Employees' responsibility towards the employer's security policies and procedures.
- Measures to perform a robust audit of those efforts.

The most successful training must be structured as an ongoing process.

5.6.2 Current State

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. As an OAG compliance item, the Microsoft BitLocker option is required to encrypt data at rest on desktops and laptops. This has not been implemented as yet. BitLocker also has specific hardware requirements, which will be addressed within the project's scope.

As an OAG compliance item, some initial policy and procedure documents are required. This policy library has not been implemented as yet.

5.6.3 Future State Recommendations

A project should be completed to implement the Microsoft BitLocker solution for all desktops and laptops. This involves enabling additional security and documenting the outcome.

Cyber awareness training should be implemented as this is an OAG compliance item. A training platform for all employees can be run as a campaign (over 3 months) once a year.

A project should be completed to implement the ICT Security Framework policy library as a staged approach over two years.

5.6.4 Budget Estimates

See the following table for an indication of ongoing costings:

Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
Cyber Incident Response Plan		$5,100		
Security Awareness Training	$462	$476	$490	$505
ICT Security Framework	$5,000	$5,000		
TOTAL	$5,462	$10,576	$490	$505

*Pricing excludes GST and is a budget estimate only. Annual price increases are predicted and subject to change.

6. Project Management

The ICT Strategic Framework identifies the key components that must be considered in managing a local government's information resources. It represents the key elements, and their relationships, that might be expected in an 'ideal' environment. In reality, the extent to which it is applicable will depend on the size and complexity of the local government.

This describes planning, organising, controlling, and managing resources to achieve specific goals. Elements to consider are as follows:

Element	Explanation
Project Initiation	The process of defining the scope of the project. This may involve establishing the scope, a project charter, and a preliminary project plan.
Project Planning	Refers to establishing a project plan detailing how a project will be accomplished within a specific timeframe and with given resources. A project plan usually identifies various project milestones and stages and the timeframes in which they are to be completed.
Project Execution	Refers to the process of carrying out or implementing the project. Project Execution is the implementation phase of the project plan and is commenced once the project planning phase is complete.
Monitoring and Controlling	Refers to monitoring the project's progress concerning the project plan and controlling resources to ensure project delivery on time and within budget.
Project Closing	The process of completing project deliverables, reviewing the project's outcome against objectives, documenting the lessons learned, archiving project records, and releasing project resources.

The elements listed above make up the Project Management component of the framework. Project Management includes one core area that should be addressed for ICT decision-making. The core area is IT Projects which is documented below. The Industry Best Practice, Current State, and Future State Recommendations are included for the core area.

6.1 IT Projects

6.1.1 Industry Best Practice

The definition of an IT project can be based on several factors but often on purchasing requirements, which is inevitably dollar value. For an IT project to be completed successfully, there are typically three documents:

- Business case – justification for work that looks at benefit, cost, and risk.
- Project statement – scope, objectives, and participants.
- Project plan – formal approval to guide execution and control.

Once an IT project has started, there usually are three phases:

- Execution – carrying out or implementing the work.
- Monitoring/Controlling – progress of the plan/resources on time/budget.
- Closing – reviewing the outcome, lessons learned, and releasing resources.

6.1.2 Current State

The Shire has completed several small and large projects in 2020 and 2021. In most projects, the previous IT provider managed the execution, monitoring, and closing of each project.

In most instances, no business case, project statement, or project plan was created. No business cases will have resulted in several projects taking longer than expected.

6.1.3 Future State Recommendations

Focus Networks recommends three IT project-related documents for future use with IT projects. The Shire should create two primary internal documents:

- A business case template to be used to help communicate the merits of a course of action to key decision makers.
- A project statement template will outline deliverables and highlight constraints, assumptions, and success factors.

The client should request one primary external document from the third party implementing the IT solution:

- A project plan documents activities, milestones, schedules, and duration.

These three documents listed above should help run a smooth project that can be officially closed by discussing the lessons learned.

6.1.4 Budget Estimates

Budget estimates are not relevant for this section.

Appendix A Microsoft Licenses

Agreement	
Program:	Microsoft 365 CSP
Customer Name:	Shire of Cocos Keeling Islands
Microsoft Tenant	67CCEA4A-AB25-439A-852F-4465D436D91A

Part Number	Product Description	Qty	Renewal Period
	Microsoft 365 Business Standard	7	Monthly
	Microsoft Defender for Office 365 (Plan 1)	38	Monthly
	Office 365 E1	3	Monthly
	Office 365 E3	32	Monthly

Part Number	Product Description	Qty	Renewal Period
	Windows Server STD CORE 2019 English LocalGovernment OLP 2Licenses NoLevel CoreLic	16	Annual
	Windows Server CAL	15	Annual
	RDS CAL	15	Annual

Appendix B Summary of Estimates

Category	Description	2022-2023 Costs	2023-2024 Costs	2024-2025 Costs	2025-2026 Costs
1.1	IT Support Arrangements	$39,652	$40,842	$42,067	$43,329
1.2	IT Risk Management	$5,000	$5,150	$5,305	$5,464
2.1	Corporate Applications	$25,988	$32,268	$27,571	$28,398
3.1	Anti-Virus	$4,032	$8,331	$8,581	$8,838
3.2	ISP Links	$14,680	$27,090	$27,903	$28,740
3.3	Uninterruptable Power Supply	$630	-	$649	-
3.4	Desktops / Laptops	$32,535	$53,571	$31,620	$28,083
3.5	Servers	$4,998	$33,168	$21,041	$21,673
3.6	IP Telephony	-	$21,875	$5,265	$5,358
3.7	Printing	-	-	$20,000	$20,000
4.1	Backups & Disaster Recovery	$9,576	$9,863	$10,159	$10,464
4.2	IT Disaster Recovery Plan	$5,670	$1,700	$1,751	$1,804
5.1	Domain	$7,755	$3,630	-	-
5.2	Internet Gateway	$3,840	$3,955	$4,074	$5,477
5.3	Computer Room	$3,500	-	-	-
5.4	Local Area Network	$8,250	$42,000	$2,040	$5,000
5.5	Patching	$8,180	$8,425	$8,678	$8,939
5.6	Cyber Response	$5,462	$10,576	$490	$505
TOTAL		$179,748	$302,445	$217,194	$222,069

FOCUS NETWORKS
WE KNOW I.T.
focusnetworks.com.au

Appendix C Computer Information

Computer Name	Current Model	Serial Number	Contact Name	Date Purchased	Proposed Replacement Year	Estimated Cost
SCKCKIBWKS1	HP EliteDesk 800 G4 DM 35W	8CC8471Z9N	environment	29/11/2018	22-23	$2,600
SCKCKIBWKS2	OptiPlex 7070	JLXHRZ2	seniorbuilder	6/11/2019	22-23	$2,600
SCKRMTALPT4	HP ProBook x360 11 G3 EE	5CG9457GG9	Aindil Minkom	12/11/2019	22-23	$3,200
SCKRMTALPT5	HP ProBook x360 11 G3 EE	5CG9457FNG	Seriwati Iku	12/11/2019	22-23	$3,200
SCKCKIALPT10	Latitude 3300	FN8KGW2	comms	26/11/2019	22-23	$3,200
MSA00758	HP ProBook x360 11 G3 EE	5CG9457DXL	Mazlan Hamiril	18/12/2019	22-23	$3,200
SCKCKIAWKS1	OptiPlex 7080	CD7HX53	debtors	21/09/2020	23-24	$2,600
SCKCKIAWKS4	OptiPlex 7080	GSTCX53	youthrec	21/09/2020	23-24	$2,600
SCKCKIAWKS5	OptiPlex 7080	GSWKX53	admin	21/09/2020	23-24	$2,600
SCKCKICWKS1	OptiPlex 7080	GSTGX53	IPRF	21/09/2020	23-24	$2,600
SCKCKICWKS2	OptiPlex 7080	CDZGX53	mfcs	21/09/2020	23-24	$2,600
SCKCKIALPT2	Latitude 5510	7BQKR73	mfcs	1/12/2020	23-24	$3,200
SCKCKIALPT3	Latitude 5510	15YKR73	apmc	1/12/2020	23-24	$3,200
SCKCKIALPT4	Latitude 5510	9HTJR73	leasing	1/12/2020	23-24	$3,200
SCKCKIALPT5	Latitude 5510	882JR73	infrastructure	1/12/2020	23-24	$3,200
SCKCKIALPT6	Latitude 5510	5QYJR73	rates	1/12/2020	23-24	$3,200
SCKCKIALPT7	Latitude 5510	CN19P73	governance	1/12/2020	23-24	$3,200
SCKCKIALPT8	Latitude 5510	F1YKR73	CDC	1/12/2020	23-24	$3,200

Computer Name	Current Model	Serial Number	Contact Name	Date Purchased	Proposed Replacement Year	Estimated Cost
SCKCKIALPT9	Latitude 5510	3FTJR73	ranger	1/12/2020	23-24	$3,200
SCKCKIAWKS2	OptiPlex 7080	FJRDL83	CSO	29/12/2020	24-25	$2,600
SCKCKIAWKS3	OptiPlex 7080	FJRJL83	creditors	29/12/2020	24-25	$2,600
SCKCKIAWKS6	OptiPlex 7080	FJMJL83	comms	29/12/2020	24-25	$2,600
SCKCKIAWKS7	OptiPlex 7080	FJTHL83	stings.register	29/12/2020	24-25	$2,600
SCKCKICWKS3	OptiPlex 7080	FJSDL83	infrastructure	29/12/2020	24-25	$2,600
SCKCKIALPT1	HP ProBook 440 G8 Notebook PC	5CD120NJFK	fmills	30/06/2021	24-25	$3,200
SCKRMTALPT2	HP ProBook x360 11 G7 Education Edition	5CG1339VTD	Ayesha	15/11/2021	25-26	$3,200
SCKRMTALPT3	HP ProBook x360 11 G7 Education Edition	5CG1339VT5	Helen	15/11/2021	25-26	$3,200
SCKCKIAWKS13	Latitude 5520	GXQ8BL3	environment	8/02/2022	25-26	$3,200
SCKCKIAWKS10	HP ProDesk 600 G6 Desktop Mini PC	8CC2150KLS	governance	19/04/2022	25-26	$2,600

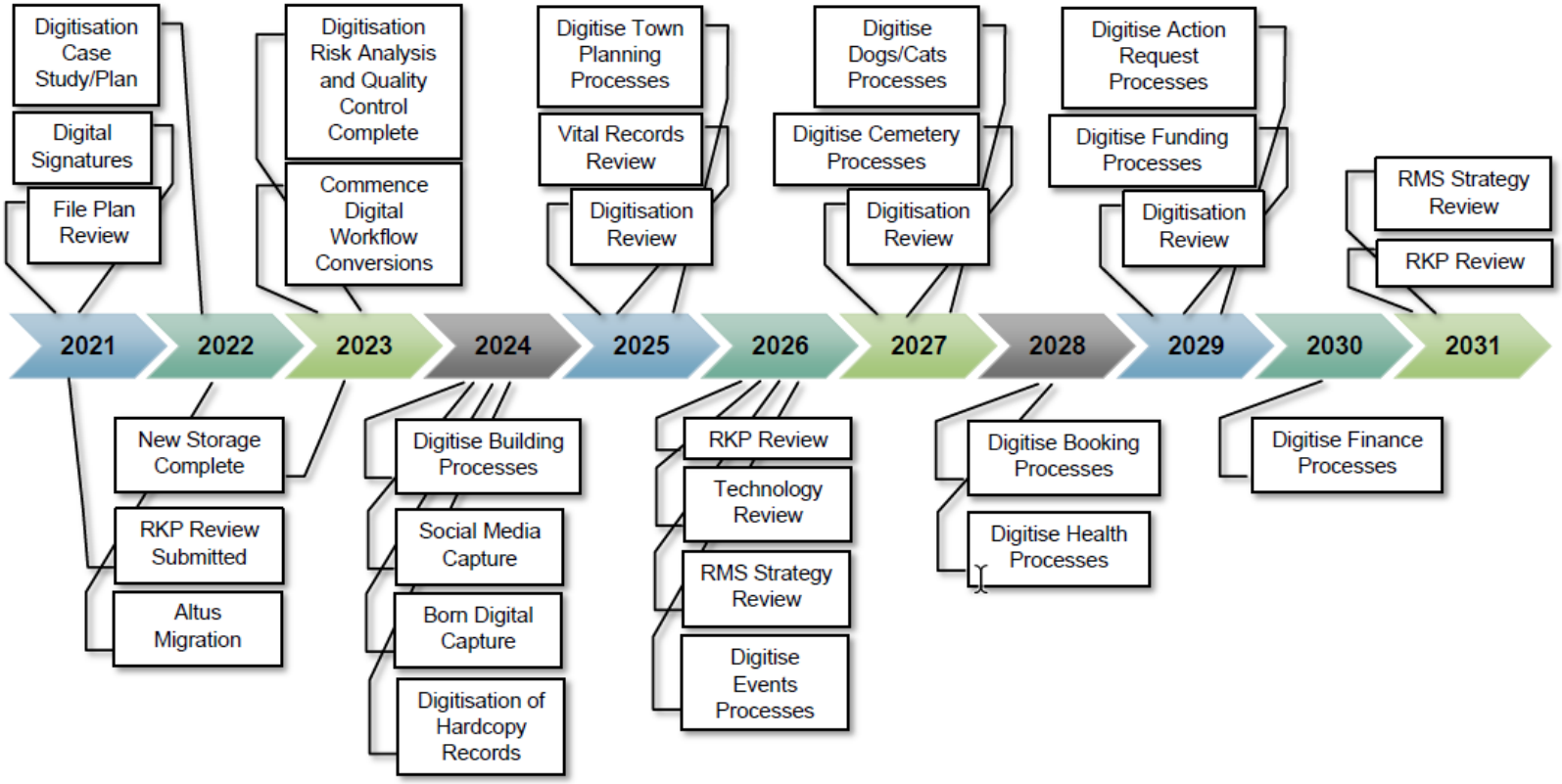
Appendix D SynergySoft License Information

Description	Qty	Total
Annual License Fee (ALF), IT Vision Software System Including the following modules: 01/07/2021	1.00	$21,984.41
Annual Licence Fees - SynergySoft per User	6.00	
Annual Licence Fee, Core Financials (Excludes Trusts)	1.00	
Annual Licence Fee, Automation Toolset – Automated Emails	1.00	
Annual Licence Fee, Easy Budgeting Tool	1.00	
Annual Licence Fee, Email Debtor	1.00	
Annual Licence Fee, Excel Integration	1.00	
Annual Licence Fee, Mapping Enquiry	1.00	
Annual Licence Fee, Payroll	1.00	
Annual Licence Fee, Purchase Ordering	1.00	
Annual Licence Fee, Rates, and Property inc Model and Pools	1.00	
Annual Licence Fee, Receipting	1.00	
Annual Licence Fee, Report Manager	1.00	
Annual Licence Fee, Workshop Management System	1.00	
12388582-UV 01/07/2021	8.00	$1,664.64
Altus Procurement	1.00	$1,631.80

Appendix E Records Management Roadmap

ROAD MAP

This roadmap is based on the assumption **Council will make funding available for consultants to assist with the development and implementation.**



Glossary of Terms

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.

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.

AGILE
Agile is an iterative project management and software development approach that helps teams deliver value to their customers faster.

Anti-Virus
Software designed to detect, stop and remove viruses and other malicious software.

AI
Artificial intelligence (AI) is a wide-ranging branch of computer science concerned with building intelligent machines capable of performing tasks that typically require human intelligence.

API
Application Programming Interface (API) - This is an interface to a computer operating system or software program that gives other programs access to functions similar to those offered to users through a graphical user interface.

Authentication
Verifying the identity of a user, process, or device is a prerequisite to allowing access to resources in a system.

Availability
The assurance that systems and information are accessible and useable by authorised entities when required.

Backup
In information technology, a backup, or data backup, is a copy of computer data taken and stored elsewhere so that it may be used to restore the original after a data loss event.

Bandwidth
Commonly used to mean the capacity of a communication channel to pass data through the track in a specified amount of time. Usually expressed in bits per second.

CAL
A Client Access License (CAL) grants specific Microsoft server software access. CALs are used in conjunction with Microsoft Server software licenses to allow Users and Devices to access and utilize the services of that server software.

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.

Content filtering
The process of monitoring communications such as email and web pages, analysing them for questionable content, and preventing the delivery of dubious content to users.

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, to improve business relationships with customers.

Deep Packet Inspection
Deep packet inspection (DPI) is a technology that allows a firewall device to classify passing traffic based on rules that not only include information about layer three and layer four 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 an 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 organization's network.

DNS
The domain name system (DNS) is how Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address, for example, www.focusnetworks.com.au.

Device Driver
A device driver is a small program that allows a peripheral device, such as a printer or scanner, to connect to a computer.

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.

Encryption
Encryption converts electronic data to an unrecognizable or encrypted form that unauthorised parties cannot easily understand.

Ethernet
Ethernet is the most widely installed local area network LAN technology. An Ethernet LAN used to use coaxial cable but these days uses unique 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 often used to transmit light between the two ends of the thread 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. Generally speaking, a firewall is a hardware device.

Firmware
A software program or instructions is programmed on a hardware device's flash ROM. It provides the necessary instructions for communicating with the other computer hardware.

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 protects the perimeter of your network. They are your first line of defence, 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. GIS enables people to see, analyze, and understand patterns and relationships more easily.

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

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 offers multiple deployment models' benefits. A hybrid cloud can connect collocation, managed, or dedicated services with cloud resources.

ICT
Information and communications technology (ICT) is an extended term for information technology (IT) that 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.

Incident Response Plan
Documenting a predetermined set of instructions or procedures to detect, respond to, and limit the consequences of malicious cyber-attacks against an organization’s information systems.

IP Address
An IP address is a 32-bit number that identifies each sender or receiver of information 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 specific 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 can take immediate action based on a set of rules established by the network administrator.

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.

ITIL
Information Technology Infrastructure Library (ITIL) - An initiative developed by the Central Computing and Telecommunications Agency consultancy for the government of the United Kingdom. It offers a set of best practices in 24 service delivery and IT service support areas, including help desk, problem management, change management, software distribution, and cost control.

HTTP
The Hypertext Transfer Protocol (HTTP) is the rule 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 standard communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building).

Latency
Sometimes called lag, it is the term used to describe delays in communication over a network.

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 direct WAN port and the secondary WAN port.

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 spyware, programming that gathers information about a computer user without permission.

Mbps
Mbps means 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 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 the point of impact to the end 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 specialized for serving files by its hardware, software, or configuration. It is often manufactured as a computer appliance – a purpose-built technical computer.

NAT
Network Address Translation (NAT) is the translation of an Internet Protocol 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 wholesale-only, open-access data network. It is based on the premise that access to fixed line, wireless, and satellite broadband connections is sold to retail service providers (RSPs), who then sell internet access and other services to consumers.

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 transmitting power to the target device at the end of an Ethernet cable by carrying capacity in the unused 4/5 and 7/8 wires. It enables access points and other remote devices to be installed without a 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 data redundancy, performance improvement, or both.

RADIUS
Remote Authentication Dial-In User Service - A security protocol transports passwords between the access device and the authentication server.

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 that 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 related to.

RPO
The time 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 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 that 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 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.

SFF
A small form factor (SFF) is a computer form factor designed to minimize the volume of a desktop computer. This term can sometimes describe physical hard disks more minor than the standard 3.5" hard drives.

SIP
The Session Initiation Protocol (SIP) is a communications protocol for signalling and controlling multimedia communication sessions. The most common SIP applications 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 standardized service contract where a service is formally defined. Particular aspects of the service – scope, quality, responsibilities – are agreed upon between the service provider and the service user. A common feature of an SLA is a contracted delivery time (of the service or performance).

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 a capability provided by specific techniques.

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 mainly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

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

Spyware
Spyware is any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (sometimes called a SpyBot or tracking software), spyware is programming 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 a Solid State Disk (SSD.) Instead, information is stored in microchips. Conversely, a hard disk drive uses a mechanical arm with a read/write head to move around and read data 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 seamlessly signing on at each method in some configurations.

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 precisely what adjacent network point the data should be sent to.

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 in which the software is tested in the "real world" by the intended audience.

UPS
An uninterruptable 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 it is restored.

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

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). VOIP 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 (a 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 organization's network.

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 enables 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 unavailable.

WiFi
A technology that allows electronic devices to connect to a wireless LAN (WLAN) network, mainly using the 2.4 gigahertz (12 cm) UHF and five 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.

WPA
Wi-Fi-protected access (WPA) is a security protocol used in Wi-Fi networks. It improves WEP because it offers excellent protection through sophisticated data encryption.