Shire of Nannup

rest • connect • grow

2025-2035

ICT Strategic Plan

ICT Strategic Plan for the Shire of Nannup (2025–2035)

1. Introduction

The Shire of Nannup, a small but vibrant rural local government in Western Australia, recognises that Information and Communications Technology (ICT) is central to delivering efficient, secure, and responsive services.

This ICT Strategic Plan aligns with the Department of Local Government, Sport and Cultural Industries (DLGSC) ICT Strategic Framework and cybersecurity best practices promoted by the Office of the Auditor General (OAG), including the adoption of the **Essential Eight**.

The Shire has adopted a **Managed Services Model** for ICT delivery to ensure access to specialist skills, improve service reliability, manage cybersecurity risk, and contain operational costs.

2. Vision

To leverage ICT through a managed services partnership to deliver efficient, secure, and accessible services, strengthening the Shire's capacity to support its community's current and future needs.

3. Strategic Objectives

3.1. Enhance Digital Infrastructure through Managed Services

- Engaged a qualified **Managed Service Provider (MSP)** to deliver core ICT infrastructure support, security monitoring, and help desk services.
- Upgraded Shire ICT assets to modern, scalable, and secure systems, with the MSP responsible for monitoring and maintenance.
- Transition appropriate services to cloud-hosted solutions to improve resilience, availability, and disaster recovery.
- Partner with the MSP to improve internet connectivity, network security, and systems performance.

3.2. Strengthen Cybersecurity and Risk Management

The Shire, supported by its Managed Service Provider, will fully adopt the **Essential Eight Maturity Model**, targeting **Maturity Level 2** by December 2025.

Actions:

- **Implement Essential Eight Controls** (with MSP support), including:
    - Application control
    - Patching applications and operating systems within 48 hours
    - Macro control and user application hardening
    - Multi-Factor Authentication (MFA)
    - Secure daily backups with full restoration testing
- **Managed Cybersecurity Services:**
    - MSP to provide 24/7 monitoring, detection, and initial response for cybersecurity threats.
    - MSP to assist in implementation and continuous improvement of Essential Eight controls.
- **Reporting Requirements:**
    - **Cyber Threat Reporting:**
        - MSP provides monthly threat detection and response reports to the Shire's Executive Management Team (EMT).
        - Significant incidents reported immediately to the CEO.
    - **Backup Success and Restoration Testing:**
        - MSP manages daily backups with automated success/failure monitoring.
        - MSP conducts full restoration tests every six months, reporting outcomes to EMT.

- **Training and Awareness:**
    - Staff and elected member cybersecurity training delivered annually, coordinated between Shire ICT leadership and MSP.
- **Audit and Monitoring:**
    - Annual external cybersecurity audits, coordinated with the MSP.

3.3. Improve Service Delivery through Digital Platforms

- Expand digital service offerings, including online payments, forms, and self-service portals.
- Enhance website accessibility and mobile responsiveness, leveraging MSP expertise.

3.4. Integrate ICT with Strategic Planning and Data-Driven Decision Making

- Integrate ICT priorities into the Corporate Business Plan and Long Term Financial Plan.
- Partner with the MSP to develop data analytics and reporting tools to assist with informed decision-making.

---

4. Implementation Plan

Note: ERP System Transition Planning is covered under section 11.

Year	Key Initiatives
Completed	Finalise Managed Service Provider agreement. Conduct ICT audit and Essential Eight gap analysis. Begin cloud migration planning.
Completed	Implement MFA and application control.
2025	Achieve Essential Eight Maturity Level 2. Conduct full backup restoration testing cycle.
2026	Launch cybersecurity training programs.
2028	Expand digital service offerings and review managed services performance.

Year	Key Initiatives
2029–35	Review technology trends, reassess managed services needs, and implement continuous improvements.

Annual Reviews:
An annual ICT review will be conducted, assessing MSP performance, Essential Eight progress, and digital service enhancements.

5. Governance

- **Executive Management Team (EMT):**
  - Provides strategic oversight of ICT services, cybersecurity, and digital transformation initiatives.
  - Receives monthly reports from the MSP covering system health, cyber threats, backup success, and incident management.
  - Responsible for escalation of significant ICT risks or breaches to the Audit and Risk Committee and Council.
- **Managed Services Agreement:**
  - Formal contract with performance KPIs covering system uptime, cybersecurity resilience, backup reliability, response times, and project delivery.
  - Reviewed annually with formal service level agreement (SLA) reviews.
- **Mandatory Reporting:**
  - **Monthly** MSP reports on cybersecurity, backup status, and system performance to the EMT.
  - **Biannual** cybersecurity and ICT health summary reports to Audit and Risk Committee.
- **Policies and Procedures:**
  - Ongoing development of ICT governance policies, jointly maintained by the Shire and MSP.

6. Budget and Resource Allocation

- ICT operating costs primarily through the Managed Services contract, Software Licencing and equipment leasing, supplemented by capital projects (hardware upgrades, new systems).
- Provision for annual cybersecurity audits, Essential Eight improvement projects, and staff training.
- Budgeting to be aligned with the Long Term Financial Plan.

---

7. Risk Management

- **ICT Risk Register:** Maintained and reviewed quarterly by EMT in consultation with the MSP.
- Key risk areas include:
    - Cybersecurity threats
    - Data loss and backup failures
    - Vendor lock-in risks
    - Service disruption risks.
- **Backup and Disaster Recovery:**
    - Managed daily backups (on-premises and cloud).
    - Full system restoration tests every six months.
    - Immediate escalation and remediation process for any backup failure or restoration failure.

7.1 Risk Assessment

The following risk assessment has been undertaken in line with the Shire of Nannup Risk Management Framework

Risk ID	Risk Description	Likelihood	Consequence	Risk Rating	Controls / Mitigations
ICT01	Cyberattack (e.g., ransomware, phishing)	4 – Likely	3 – High	High	Firewall & antivirus; Staff training; Regular backups; Incident response plan. Implementation of OAG approved Essential 8. Managed Services Model for ICT delivery to ensure access to specialist skills, improve service reliability, manage cybersecurity risk.
ICT02	Data loss due to hardware failure	3 – Possible	2 – Medium	Medium	Cloud backups; RAID storage; Hardware refresh schedule, Datto Platform.
ICT03	Unauthorized access to systems (internal or external)	3 – Possible	3 – High	High	Role-based access control; MFA; Audit trails. Managed Services Model for ICT delivery to ensure access to specialist skills, improve service reliability, manage cybersecurity risk.
ICT04	Extended network outage / connectivity failure	2 – Unlikely	2 – Medium	Medium	Redundant internet connections; SLA with ISP; UPS for networking hardware.
ICT05	Breach of data privacy / Personal information disclosure	2 – Unlikely	3 – High	Medium	Data encryption; Privacy policy compliance; Staff confidentiality agreements. Managed Services Model for ICT delivery.
ICT06	Failure of core business application (e.g., financial, records, asset system)	3 – Possible	2 – Medium	Medium	Vendor SLAs; Regular updates and patching; User training and documentation.

Risk ID	Risk Description	Likelihood	Consequence	Risk Rating	Controls / Mitigations
ICT07	Loss of access to email or communications systems	2 – Unlikely	2 – Medium	Medium	Microsoft 365 monitoring; Backup systems; Communication protocols. Managed Services Model for ICT delivery to ensure access to specialist skills, improve service reliability.
ICT08	Inadequate ICT policy or outdated procedures	3 – Possible	1 – Low	Low	Regular policy reviews; Compliance audits
ICT09	Lack of staff ICT skills or awareness	4 – Likely	2 – Medium	High	Ongoing ICT training; Cyber security awareness programs; Onboarding process. The Shire has adopted a Managed Services Model for ICT delivery to ensure access to specialist skills, improve service reliability, manage cybersecurity risk, and contain operational costs.
ICT10	Environmental impact due to e-waste mismanagement	2 – Unlikely	1 – Low	Low	E-waste recycling program; Vendor take-back schemes; Procurement policies.

8. Business Systems and Applications

8.1. Core Business Applications

The Shire uses a variety of software tools to support its core business and administrative functions:

- IT Vision SynergySoft: This is the principal finance system used by the Shire for managing financial operations and ratepayer interactions.
- Microsoft Office 365: Provides productivity and collaboration tools including Word, Excel, Outlook, and Teams.
- MS Project: Used for project planning and management.
- Monday.com: Utilized for task and project tracking.
- Nitro PDF & Foxit PDF: Applications for managing PDF documents, including editing and conversions.

8.2 Infrastructure and ICT Environment

- The Shire operates a hybrid environment including both on-premise and cloud-based infrastructure:
- Servers: One Dell Hyper-V server located onsite at the Administration Office.
- Network Equipment:
- Aruba Switches (3 units)
- Fortinet FortiGate Firewalls (1 at Admin Office, 1 at Depot)
- Aruba Central Wireless Access Points (WAPs): 2 at Admin Office, 1 at Depot
- Endpoints:
- Dell Latitude laptops and Dell OptiPlex desktops used by staff.
- Fujifilm and Brother multifunction devices for printing and scanning.
- All key hardware components, including firewalls, switches, WAPs, and endpoints, are on lease and relatively new.

8.3 Communication Systems

- RingCentral VoIP: Managed by a third-party provider for internal and external voice communications.

8.4 Cloud Services and Licensing

- Microsoft 365 Licensing: Managed through Crayon, with Managed Service Provider (MSP) access to the Crayon portal for license administration.
- Backup and Disaster Recovery:
- DATTO SIRIS: Used for data backup and disaster recovery, managed via Frontline Services.
- MSPs are given administrative access for maintenance and monitoring.

8.5 Security Systems

- The Shire has implemented strong cybersecurity practices with the following systems:
- Microsoft Defender ATP: Provides advanced threat protection across endpoints.
- Dell SecureWorks MDR: Utilized for Managed Detection and Response, helping detect and respond to cyber threats.

8.6 Support and Service Structure

- ICT support services are structured around:
- Help desk and technical support (onsite and remote)
- Monthly on-site visits
- Proactive maintenance
- SLA-based response times (tiers based on incident urgency)
- Ongoing strategy, documentation, and compliance reporting

8.7 Facilities Requiring ICT Support

- Administration Building (Adam St): Main location, housing 22 staff.
- Works Depot (Kearney St): Secondary location, supporting 3 staff.

8.8. Additional Applications and Documentation

- ICT Documentation: MSP is required to maintain all IT documentation.
- Cybersecurity Reporting: Includes maturity assessments against the ASD Essential Eight framework.
- Disaster Recovery Planning: Includes annual reviews and updates in collaboration with Shire staff.

9. Emerging Trends and Technologies

9.1 Cloud Computing and Hybrid Infrastructure

Opportunity:

- Increased flexibility and scalability: Moving services like data storage, communications, and applications to the cloud enables cost-efficient scalability as needs grow or shift.
- Business continuity: Enhanced disaster recovery and remote access capabilities ensure continuity during crises or natural disasters.

Challenge:

- Data sovereignty and privacy: Local governments must ensure data remains compliant with Australian privacy laws.
- Migration complexity: Legacy system data cleansing and conversion (as outlined in the RFQ) can be resource-intensive and risky.

9.2 Cybersecurity and Threat Intelligence

Opportunity:

- Advanced tools like Microsoft Defender ATP and Dell SecureWorks MDR (already in use by the Shire) improve detection and response to threats.
- Alignment with ASD Essential Eight: Allows structured improvement of cyber maturity across systems.

Challenge:

- Evolving threat landscape: Increased ransomware and phishing attacks demand ongoing investment and staff training.
- Security skills shortage: Local governments often struggle to recruit or retain cybersecurity professionals.

9.3 AI and Automation

Opportunity:

- Help desk automation (e.g., chatbots) and AI-driven analytics can reduce operational workload, improve service delivery, and assist with proactive infrastructure management.
- Predictive maintenance: AI can forecast infrastructure failure before it happens, saving costs and downtime.

Challenge:

- Ethical and privacy concerns: AI must be implemented with strong governance to protect public data.
- Technical complexity: Requires new capabilities and integration with existing platforms.

9.4 Mobility and Remote Work Support

Opportunity:

- Digital workplace services (included in the Shire's scope of work) support hybrid and remote work models, increasing workforce flexibility and satisfaction.
- Endpoint management tools facilitate secure access from various locations and devices.

Challenge:

- Increased risk exposure: More devices and remote users increase the attack surface.
- Bandwidth and infrastructure upgrades: Remote support places strain on existing network infrastructure.

9.5 Data Governance and Compliance

Opportunity:

- Centralised ICT documentation and regular DRP reviews (as required by the Shire) support strong governance and regulatory compliance.
- Improved transparency and audit readiness align with Office of the Auditor General (OAG) standards.

Challenge:

- Volume and variety of data makes compliance complex.
- Lack of mature frameworks in some local councils can delay implementation.

9.6 Smart Community Initiatives (IoT, Sensors, Data Analytics)

Opportunity:

- Smart infrastructure (e.g., environmental sensors, asset tracking) can provide data for decision-making and improve service efficiency.
- Integration with GIS and operational platforms supports urban planning and environmental monitoring.

Challenge:

- Integration with legacy systems can be technically challenging.
- Security vulnerabilities in IoT devices if not properly managed.

9.7 Managed Services and Vendor Ecosystem

Opportunity:

- The Shire's move toward Managed ICT Services reflects a broader trend of leveraging external expertise for cost savings and improved service levels.
- Vendor collaboration can accelerate the adoption of best practices and new technologies.

Challenge:

- Over-reliance on third parties can reduce in-house knowledge and control.
- Vendor lock-in and contractual complexities may limit flexibility over time.

9.8 Sustainable ICT Practices

Opportunity:

- Equipment leasing (as done by the Shire) and cloud-based operations reduce e-waste and carbon footprints.
- Energy-efficient infrastructure aligns with sustainability targets and community expectations.

Challenge:

- Upfront investment in sustainable solutions can be higher.
- Measuring and reporting environmental impact of ICT is still evolving.

10. Business Continuity

The following measures are identified as addressing ITC Business continuity for the Shire of Nannup.

Category	Action	Purpose
Data Backup & Recovery	Implement automated daily off-site and cloud-based backups	Ensure data is restorable in case of data loss, ransomware, or server failure
Data Backup & Recovery	Conduct regular backup integrity tests	Validate that backups are working and restorable
Cybersecurity Measures	Maintain updated antivirus, endpoint protection, and firewalls	Prevent and detect malicious attacks
Cybersecurity Measures	Enable Multi-Factor Authentication (MFA) for all critical systems	Reduce the risk of unauthorized access
Cybersecurity Measures	Provide regular cyber security awareness training	Ensure staff can recognize phishing and social engineering attacks
Disaster Recovery Planning	Develop a documented ICT Disaster Recovery Plan (DRP)	Guide IT recovery during major ICT incidents
Disaster Recovery Planning	RTO (Recovery Time Objective): The maximum acceptable amount of time that a system, application, or process can be down after a disaster before significant impact occurs. It defines how quickly you need to restore operations. RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time. It defines how much data you can afford to lose, typically in terms of the time since the last backup	Prioritize restoration based on business impact
Disaster Recovery Planning	Conduct annual disaster recovery drills	Practice response to minimize confusion during real events

Category	Action	Purpose
Infrastructure Resilience	Use redundant internet connections and failover systems	Maintain connectivity during ISP or hardware outages
Infrastructure Resilience	Maintain uninterruptible power supplies (UPS) and surge protection	Ensure continuity during short-term power failures
Infrastructure Resilience	Regular hardware maintenance and asset refresh cycles	Reduce risk of system failure due to aging infrastructure
Cloud and Remote Access	Migrate critical services to secure cloud environments	Improve availability and flexibility in the event of office access disruption
Cloud and Remote Access	Enable secure remote work capability with VPN and MDM	Support business continuity during pandemics or facility closures
System Monitoring & Alerts	Implement 24/7 system and network monitoring	Early detection of failures or breaches
System Monitoring & Alerts	Set up automated alerts for system failures and anomalies	Enable rapid response to ICT events
Incident Management	Maintain an ICT Incident Response Plan (IRP)	Clearly define how incidents are reported, escalated, and resolved
Incident Management	Establish an ICT incident log and root cause analysis process	Improve response and learn from past disruptions
Vendor & SLA Management	Ensure third-party providers have continuity provisions	Protect against external supplier failure
Vendor & SLA Management	Maintain up-to-date SLAs with recovery commitments	Hold vendors accountable for system availability
Communication & Coordination	Maintain contact list for key ICT stakeholders	Ensure effective communication during disruptions
Communication & Coordination	Predefine internal and public communication strategies	Avoid misinformation and manage reputational risk

11. ERP System Transition Planning

11.1 Current State

The Shire of Nannup currently uses **Synergysoft**, provided by **ReadyTech**, as its Enterprise Resource Planning (ERP) system.

Synergysoft supports all core local government functions including:

- Property and Rating
- Financial Management (General Ledger, Bank Reconciliation, Creditors, Debtors, Assets)
- Payroll and Human Resources
- Purchasing and Plant Management
- Customer Service
- Building Services
- Works Costing
- Animal Registrations (Dogs, etc.)

ReadyTech has committed to supporting Synergysoft until at least **June 2030**. After this date, updates and official support will cease, necessitating a full system transition.

11.2 ERP Transition Strategy

The ERP system is a mission-critical platform for the Shire's operations.

A structured approach will be used to select, procure, and implement a new ERP solution aligned with the Shire’s future needs.

11.3 Key Steps and Timeline

Year	Key Actions
2026	Initiate internal review of current Synergysoft use, identify pain points and future requirements.
2026	Undertake market research on Local Government ERP solutions. Conduct site visits or case studies of other regional Councils.
2027	Prepare ERP Business Case and Options Analysis, incorporating cost-benefit assessment and risk analysis.
2028	Commence formal procurement process (Expression of Interest, Request for Tender) for a replacement ERP system.
2028	ERP system selection and contract award.
2029	Commence data migration planning and system configuration. Begin parallel run and training programs.
Early 2030	Complete go-live of new ERP system. Decommission Synergysoft post-successful transition.
Mid 2030	Conduct post-implementation review and lessons learned workshop.

11.4 Governance and Risk Management

- Executive Management Team (EMT) to oversee the ERP Transition Program.
- Establish an Internal ERP Project Team comprising Finance, Rates, Customer Service, Building, and ICT representatives.
- Engage external specialist consultants as needed for:
    - Business process mapping
    - Data migration planning
    - System integration assessments
- Strict project management controls will be applied including:

- Stage gate approvals (at Business Case, Procurement, and Implementation phases)
- Project risk register with monthly reviews
- Budget tracking and reporting to EMT and Council

- Contingency plans developed in case of delays in ERP implementation to avoid any operational disruption post-June 2030.

11.5 Critical Success Factors

- System selected must meet Western Australian Local Government regulatory requirements.
- Strong integration with financial management, rates, and compliance reporting needs.
- High data security and cloud capability (preferably SaaS/cloud-hosted solutions).
- Modern user interfaces and mobility support (field access for inspections, works crews, customer service).
- Ability to scale with Shire growth and adapt to evolving regulatory requirements.
- Vendor proven track record supporting rural and regional councils.

Conclusion

By adopting a Managed Services Model, the Shire of Nannup will gain access to specialised ICT expertise, stronger cybersecurity defences, and reliable, future-ready systems. This approach ensures that the Shire can deliver modern, resilient, and efficient services to its community in a cost-effective manner.

Furthermore, the Shire of Nannup has adopted a comprehensive suite of modern systems and applications to manage its ICT functions efficiently. The strategic use of cloud services, cybersecurity tools, and managed services supports both daily operations and long-term planning. Continued improvements through regular review, vendor management, and alignment with industry standards ensure robust support for the Shire's services and staff.

By embedding the ERP transition into this ICT Strategic Plan, the Shire demonstrates its commitment to strong digital governance, community service innovation, and operational resilience.

12. Document Control:

Date:	OCM Ref. #	Comment	Next Review	ECM Reference #
30/04/2025	N/A	Draft Plan prepared by EMCS. To be subject to a Council Report and determination no later than 30 June 2025.	N/A	