IT Assessment

Township of White River

December 16, 2022

270 BRUCE STREET, SAULT STE.MARIE, ON P6B 1P6

IT Services, Intrusion Detection, Alarm, Telecom

Contents

1. Introduction

1.1. About the Township of White River

The Township of White River is situated along Highway 17 in Northern Ontario between Thunder Bay and Sault Ste Marie. With a population of approximately 900 people, the Township is responsible for providing its citizens with all basic services and programs, including fire, landfill, recreation, and library. This requires the Township to run an efficient and reliable operation that is dependent on a solid technology framework.

1.2. Assessment Objectives

The purpose of this document is to provide findings and recommendations for the Information Technology (IT) Assessment commissioned by the Township of White River via RFP and awarded to ATS on July 28, 2022.

1.3. Methodology

ATS follows the well-known Gartner application and system fitness methodology. It evaluates primary and secondary types of business and technical data by conducting a fitness assessment. Data is prepared, collected, assessed, and rated, then analyzed with recommendations.

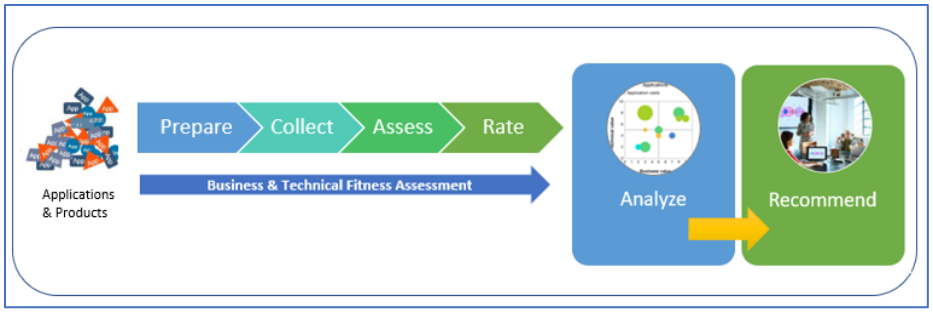

Figure 1 **Data Fitness Assessment** (Source: Adapted from Gartner, 2018)

1.4. Onsite Stakeholder Reviews

In addition to the physical, onsite assessment of rooms and equipment, stakeholder interviews were held with key resources to gather information regarding strategic and tactical components of their work and day-to-day tasks at the Township of White River. Stakeholders interviewed include the following:

- Marilyn Parent-Lethbridge – Acting CAO
- Troy Sauriol – Financial Assistant/IT (has since left the Township)
- Kim Morgan – Deputy Clerk
- Renee Berube – Administrative Assistant/IT

Township staff for the library, water treatment plant, tourist information centre, arena and fire department also participated by providing written responses to specific questions prepared by ATS.

Stakeholder feedback was incorporated into the following assessment and recommendations.

2. Executive Summary

2.1. Key Observations

Analysis of the physical results and stakeholder interviews uncovered key themes at the Township, which can be broken down into three categories:

2.1.1. Technology

- Outdated infrastructure, including equipment past end of life
- Minimal to no network protection; cyber security gaps
- Physical issues with onsite server
- Decentralized technology management

2.1.2. Processes

- Substandard policies and processes to protect network
- Decentralized IT processes and procedures, including onboarding, provisioning and offboarding of employees

2.1.3. People

- No centralized access to knowledge base or training; lack of documentation
- Lack of cyber security awareness and basic technology training
- No centralized point of contact for technology related issues
- Lack of technology oversight at the Township

2.2. Summary of Issues and Recommendations

The table below summarizes the issues and recommendations of the assessment. Further details can be found within the following sections.

ISSUE	PRIORITY	DESCRIPTION, RECOMMENDATION
INFRASTRUCTURE		
Cyber Security - Network Protection	1-High	There is an immediate need to install network protection to reduce the risk of the Township.
Cyber Security - Endpoint Protection -	1-High	There is an immediate need to install or update antivirus on end-user devices to protect and to reduce the risk of the Township.
Phone System	1-High	The Township uses an outdated, unsupported Toshiba phone system that poses issues in connecting, transferring, and dropped calls. A replacement is highly recommended.
Physical Location of Equipment	2-Medium	The current server that holds all municipal data, including the general ledger and tax information is located in an office with full physical access, allowing unobstructed access to the main revenue source of the Township. Additionally, implementing

ISSUE	PRIORITY	DESCRIPTION, RECOMMENDATION
		cable management will reduce potential safety hazards and points of failure.
Physical Security	1-High	No auditable access to the Township's main building to secure the Township assets. No audit trail for granting access where needed.
BUSINESS CONTINUITY		
Business Continuity – Back up and Recovery	1-High	In the event of a loss of the main server, recovery of customers' data will be difficult to achieve. The Township should implement best practice backup and recovery processes.
Cyber Security Insurability	1-High	Due to the infrastructure, network, and endpoint security issues the Township lacks the ability to secure cyber insurance. Cyber insurance requires the ongoing update of security devices and processes.
TECHNOLOGY SUPPORT		
IT Resources	1-High	With the departure of the former IT resource, Township staff does not have a dependable "go to" person for day-to-day IT support. There is an immediate need for IT helpdesk support.
Training	2-Medium	Multiple comments were received on the need for basic computer training and job function resources. This can be coupled with an IT helpdesk for support, including access to a repository of training material.
TECHNOLOGY STRATEGY & MANAGEMENT		
IT Leadership	2-Medium	As the Township grows and expands, so will the reliance on technology. Technology investment should be strategic. Consider investing in technology leadership in the form of a virtual CIO to help guide and make recommendations around technology decisions.
Underutilization of Microsoft 365 (M365)	2-Medium	As the Township owns Microsoft 365 licenses, it is not fully deployed and used. There is an opportunity for cost efficiencies to fully utilize M365 for email, collaboration, and addressing 'work-from-home' needs.

3. Site Assessment Details

3.1. Main Server Room

The objective is to provide an assessment of the main server room, to highlight any deficiencies found and suggest corrective actions where required. There is not a defined server room, as equipment is placed throughout the facility. However, for definition purposes “the server room” will be the janitorial room where the ISP router, main switch and phone system PBX are located.

3.1.1. Architectural Inspection

General Observations	• The wall construction is mixed between drywall and brick. • There is only one access door to this room. • There is no T-bar ceiling. • The floor is bare concrete. • The ambient temperature inside the room is adequate for the equipment.
Issues	The room is used for storage as well as the main electrical room, with access from the main lobby. • Equipment is located within the restricted area (36”) in front of an electrical panel and should be moved. • Old equipment, wiring and boxes are stored together in the same space. This presents a trip hazard and should be removed.
Mitigation Actions	• Equipment should be in a dedicated area, with restricted access. • Mandatory space of at least 36” should be kept in front of electrical panels. • Clean area to prevent fire and trip hazards.
Potential Solutions and Costs	• Maintain a dedicated equipment room by relocating non-related items to a separate storage area – no cost • Restrict access via installation of access control on one door with fob/key panel: approximately $2,500 per door (depending on door type)

3.1.2. Electrical

General Observations	• Equipment is plugged into a daisy-chained power bar setup, which does not meet standards.
Issues	• Power bars are not mounted. • No power backup system in place. • There are many boxes and unused equipment located in the area; this could become a fire hazard.
Mitigation Actions	• Install a wall receptacle on a dedicated circuit and remove power bars • Remove equipment not in production and clean area
Potential Solutions and Costs	• Remove old equipment – no cost • Install a wall receptacle on a dedicated circuit – approximately $1000-$2000

3.1.3. Fire-Detection Systems

General Observations	• There is no fire detection system or devices in the server room. Due to the nature of equipment (generating heat), early smoke/heat detection is a standard for equipment rooms.
Issues	• There is no fire suppression system. • There is no fire detection system. • There is no fire alarm pull station. • There is no fire alarm horn, bell, or strobe light. • There is no temperature monitoring of equipment.
Mitigation Actions	• An early warning heat/smoke detection system should be implemented. • A high temperature monitoring system should be implemented.
Potential Solutions and Costs	• Monitoring is included in the recommended burglary system. See section 3.4.1 for details.

3.1.4. Communication Infrastructure

General Observations	• The communications infrastructure consists of copper cable, mostly CAT5 ft6.
Issues	• Cabling throughout the building is not up to current standards. Several runs of CAT5 have been observed hanging from the ceilings, taped to floors, or running exposed in high transit areas. • Data terminations are completed in a non-uniform or non-standardized manner. Some of the terminations are broken or in poor condition. • A 5-port switch is being used as an extender for a data run which adds an unnecessary additional point of failure and network access. • Lack of equipment racks, whereby proper grounding is not observed.
Mitigation Actions	• A new data infrastructure with proper cable management is recommended. This includes use of CAT6 cables and terminations to increase network throughput and scalability. Install at least two data jacks per workstation or printer, as well as data runs for future access point implementation. • Installation of proper CAT6 patch panels with proper grounding is recommended.
Potential Solutions and Costs	• A new data infrastructure (estimated 20 drops and equipment, patch paneling, cable management) is approximately $5,000 (two weeks); roughly $200 per station.

Photos are provided below

Server Room

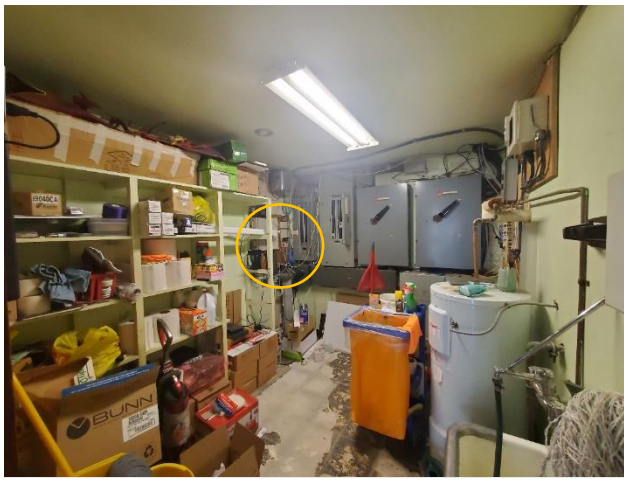

Figure 2 Main Router and Switch

Figure 3 Main Router and Switch (zoomed in)

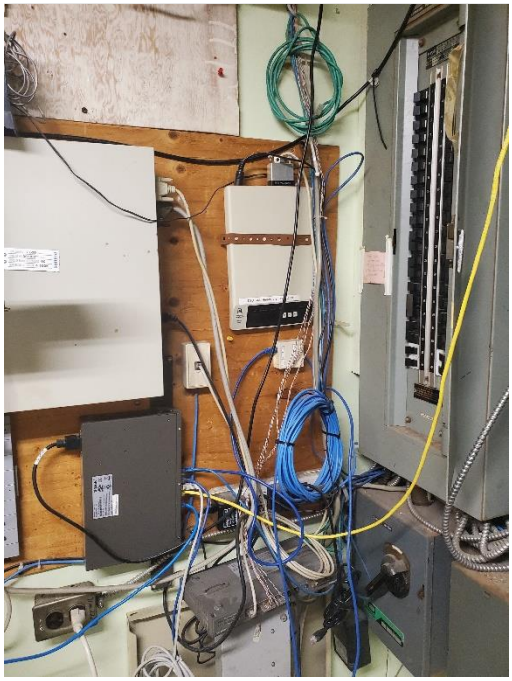

Figure 4 Power setup

Communications Installation

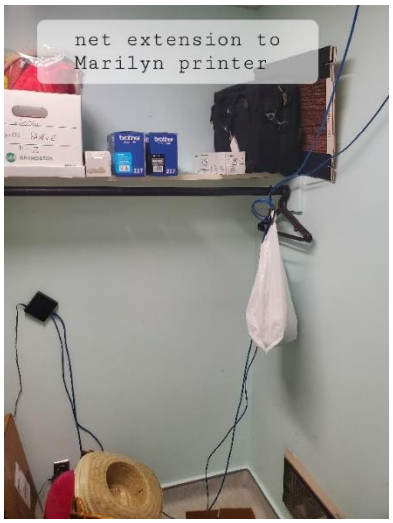

Figure 5 Switch Used as a Network Extender

Figure 6 Front Desk Network Connections

Figure 7 Non-standard cable run

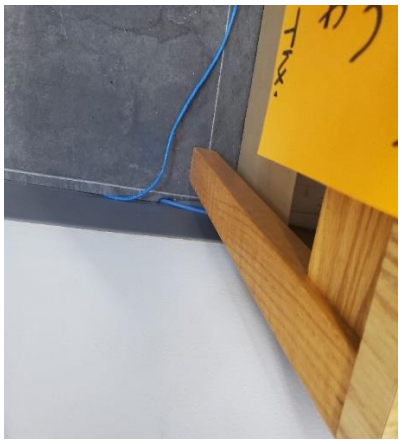

Figure 8 Non-standard cable run

3.2. Remote Sites

3.2.1. Library

General Observations	• Devices are connected through Wi-Fi. • The library has two staff computers and three public access computers. • The library has four printers, and three iPads for public usage.
Issues	• Like the main building, the library infrastructure relies solely on the ISP router for ethernet and Wi-Fi. There is no network isolation other than that provided by the router, and there is no firewall/antivirus. This is an issue as this does not provide data security for potentially sensitive information held within a library management system and for unauthorized access to the network, with a lack of password protection policies. • Frequent ISP outages.
Mitigation Actions	• Integrate and strengthen Wi-Fi access point infrastructure as a part of the main building's network • Centralize printers under the same domain as computers • Reduce the printer footprint based on usage to reduce maintenance and support costs • Provide either individual or centralized power backup/surge protection for devices
Potential Solutions and Costs	• Installation of Wi-Fi access points to isolate the public access network and harden the network; approximately $2500 • Centralized domain of printers and computers; included in Azure AD cost of M365 • Upgrade end user devices (e.g. computers and printers) to current standards to enable network protection and monitoring • Individual device power backup and surge protection; approximately $375 per workstation

Photos are provided below.

Figure 9 Library Router

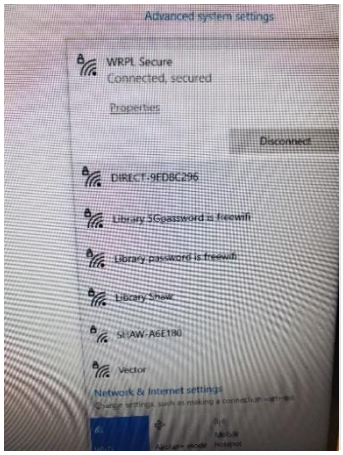

Figure 10 Wi-Fi Network SSID

Figure 11 Library Back Desk

Figure 12 Library Front Desk

Figure 13 Library Printer (Publicly Accessible)

3.2.2. Water Treatment Plant

General Observations	At the time of inspection, it was not possible to gain access to this facility; however, based on the initial interview and stakeholder responses to the ATS questionnaire, it is set up as follows: • One phone line • Shaw internet with Wi-Fi • One desktop used for Supervisory Control and Data Acquisition (SCADA) • One desktop brand new still in box, spare for SCADA There is no backup ISP solution along with device protection.

Issues	• An internet outage will be critical to SCADA system monitoring (e.g., pump fails) and there is no ISP backup solution. The Township is at risk as the water tank reserve flow is controlled by the SCADA system. • A phone line outage will be critical as it is used for the SCADA dialer. • The computer does not have UPS/surge protection. • The computer does not have antivirus. • The computer is not part of a centralized domain/access control entity. • The phone line is not integrated to the main system. • The computer is not integrated to a network access control. • No method to track activity in or out of the facility
Mitigation Actions	• Provide an ISP failover solution with a GSM router, independent from the main ISP • Integrate the phone line into the main building system • Install a UPS with surge protection • Install computer antivirus software • Upgrade computer to current standards to enable network protection; with upgrade to solid state drive (SSD) • Implement a network access control system and integrate this and any other corporate computers • Add a CCTV camera system linked to the overall Township CCTV • Install key fob system integrated to the overall Township Access Control system
Potential Solutions and Costs	• Independent ISP failover solution with a GSM router; $900 + monthly cost • Phone line integrated with main building; based on the overall on-premises phone solution; see section 3.4.2 • UPS installed with surge protection; approximately $500 • Computer antivirus (endpoint protection) software; see section 3.3.3 • Upgrade computers to SSD • Add a CCTV camera system linked to the overall Township CCTV: Approximately $1800 • Install key fob system integrated to the overall Township Access Control system: Approximately $2500

3.2.3. Tourist Information Office

General Observations	At the time of inspection, it was not possible to gain access to this facility; however, based on the initial interview and stakeholder responses to the ATS questionnaire, it is set up as follows: • One desk computer with Wi-Fi and separate ISP • One phone line
Issues	• The computer does not have antivirus software. • The computer is not part of a centralized domain/access control entity. • No method to track activity in or out of the facility
Mitigation Actions	• Integrate the phone line into the main building phone system • Install a UPS with surge protection • Install computer antivirus software • Integrate the computer to the main domain controller • Upgrade computer to current standards to enable network protection; with solid state drive (SSD) • Add a CCTV camera system linked to the overall Township CCTV • Install key fob system integrated to the overall Township Access Control system
Potential Solutions and Costs	• Independent ISP failover solution with a GSM router; $900 + monthly cost • Phone line integrated with main building; based on the overall on-premises phone solution; see section 3.4.2 • UPS installed with surge protection; approximately $500 • Computer antivirus (endpoint protection) software; see section 3.3.3 • Upgrade computers to SSD • Add a CCTV camera system linked to the overall Township CCTV: Approximately $1800 • Install key fob system integrated to the overall Township Access Control system: Approximately $2500

3.2.4. Arena

General Observations	At the time of inspection, it was not possible to gain access to this facility; however, based on the initial interview and stakeholder response to the ATS questionnaire, it is set up as follows: • One phone line (analog) • There are no computers, physical access control or CCTV (cameras) onsite
Issues	• The phone line is not integrated into the main building • No method to track activity in or out of the facility
Mitigation Actions	• Integrate the phone line into the main building phone system • Add a CCTV camera system linked to the overall Township CCTV • Install key fob system integrated to the overall Township Access Control system
Potential Solutions and Costs	• Phone line integrated with main building; based on the overall on-premises phone solution • Add a CCTV camera system linked to the overall Township CCTV: Approximately $1800 • Install key fob system integrated to the overall Township Access Control system: Approximately $2500

3.2.5. Fire Hall

General Observations	At the time of inspection, it was not possible to gain access to this facility; however, based on the initial interview and stakeholder response to the ATS questionnaire, it is set up as follows: • One phone line • Shaw internet with Wi-Fi • Keypad entry system • Computer
Issues	• An internet outage will be critical, and there is no ISP backup solution. • A phone outage will be critical. • The computer does not have antivirus. • The computer is not part of a centralized domain/access control entity.

Mitigation Actions	• Provide an ISP failover solution with a GSM router independent from the main ISP • Integrate the phone line into the main building phone system • Install computer antivirus software • Integrate the computer(s) to the main domain controller • Upgrade computer to current standards to enable network protection; with upgrade to solid state drive (SSD) • Add a CCTV camera system linked to the overall Township CCTV • Replace keypad with a key fob system integrated to the overall Township Access Control system
Potential Solutions and Costs	• Phone line integrated with main building; based on the overall on-premises phone solution • Upgrade computers to SSD • Add a CCTV camera system linked to the overall Township CCTV: Approximately $1800 • Install key fob system, to replace keypad, integrated to the overall Township Access Control system: Approximately $2500

3.3. Networking and Security

3.3.1. WAN Design

General Observations	• The main building has a simple configuration. An ISP router is connected directly to a 16-port switch. All devices either connect to this switch or wirelessly to the ISP router. • The entire network runs on one subnet 192.168.0.x with no reserved or static IP addresses.
Issues	• No firewall, meaning no network protection from unwanted internet access, leaving the network vulnerable to attacks. • The internet service is often affected by the weather, leaving the main building without communications until service is restored, impacting productivity.
Mitigation Actions	• Install a firewall. A firewall will allow the network traffic to be monitored and filtered, to help prevent malicious actors from accessing the internal network. Newer firewalls include an antivirus

	solution, adding a layer of protection from malware, spyware, and other malicious programs. • Implement a failover plan with a secondary ISP and load balancing router, to enable seamless switching between ISPs should an outage occur, keeping critical systems online and minimizing impact to customers and staff productivity.
Potential Solutions and Costs	• Install a firewall - $1500-$4000 • Install a secondary ISP for failover – an approximate one-time fee of $1000 plus monthly fees starting at $25 based on usage

3.3.2. Active Directory

General Observations	• Active directory runs on the main server, with only five active users.
Issues	• Currently, the server hosting the Township's entire operating system including general ledger and tax software is completely unsecured. This means that anyone can simply walk up to the server and gain domain admin privileges, granting them unrestricted access to all domain-joined machines as well as stored information.
Mitigation Actions	• With an existing Active Directory Domain already in place, and existing Microsoft 365 (M365) licenses, we recommend migrating to a cloud-based Azure Active Directory setup. This will allow all machines to be centrally managed, while also allowing users to sign into their machines and the M365 suite with the same credentials. This will also allow using a cloud-based VPN setup, so users can access on-premises applications securely from home or other remote locations.
Potential Solutions and Costs	• Azure Active Directory $8.22 user/month (included in M365 license)

3.3.3. Security

General Observations	• There is no password policy in place. • Emails are reused by employees • There is minimal, expired endpoint antivirus.

	• There is minimal malware detection on the server and nothing on end user devices; therefore, any malicious software can make it onto an endpoint and can compromise the network. • There is no firewall protection, leaving the network vulnerable through open ports. A firewall will secure the network from unwanted internet traffic and access.
Issues	• Each employee writes all his/her passwords on paper, which goes into a closed envelope which is stored in the vault. • Each employee has a key to the vault; there is no record of keys, and they use the honour system when leaving the company. • There is no log of accesses to the vault. • No network protection, due to the lack of a firewall, lack of effective endpoint antivirus protection and lack of effective malware detection. • The Township lacks the ability to secure cyber security insurance (further mitigating the risk of cyber attacks and ensuring business continuity for the citizens of White River) due to these open issues.
Mitigation Actions	• Implement a password policy. As per guidance from the Government of Canada, Canadian Centre for Cyber Security and industry best practices, it is recommended to implement a password policy requiring passwords to be at least 12 characters long and encouraging passphrases of 4 or 5 random words that meet the 12-character minimum. It is also recommended to blacklist common and insecure passwords. • Utilize a password manager. A password manager would allow for both the generation of secure passwords and passphrases, and the secure sharing of passwords between employees. • Install endpoint antivirus. Endpoint antivirus is the last line of defense for a computer network, protecting against known viruses. If a virus makes it through all other protections and ends up on an endpoint (laptop, desktop, server), an endpoint antivirus will detect it, isolate the file and remove the virus before it can compromise the machine. • Install ransomware detection. Ransomware detection analyzes behaviour within the network and can protect against unknown threats. • Install a firewall to protect the network against unwanted access.

Potential Solutions and Costs	• Password Managers:
	  ○ Dashlane - $6.76/user
	  ○ Bitwarden - $4.05/user
	  ○ Nordpass - $4.85/user

	• Endpoint Antivirus:
	  ○ MalwareBytes - $94.53/device/year
	• Ransomware Protection:
	  ○ Approximately $1.98 per device
	• Firewall:
	  ○ Cost ranges $1500-$4000

3.3.4. Logical Network Design

3.3.4.1. Wireless Environment

General Observations	• The Township of White River does not have a wireless infrastructure in place and relies solely on the ISP router for both employees and guests.
Issues	• As some computers connect to the main domain through the ISP router's Wi-Fi, they might be vulnerable to attacks or even unauthorized access from the exposed network.
Mitigation Actions	• Install a system with wireless access points on a secured network for domain computers and an isolated network for public usage.
Potential Solutions and Costs	• Wireless secured network isolated from the public; approximately $1,900 per access point installed with 5-year support.

3.3.4.2. Systems and Storage

General Observations	• The Township of White River has a main server located inside an office. This machine serves as a file server, database server and web server for all municipal data and iCity applications. • Users save documents to their local computer drive, not always on the network (p: drive). • The server is running Windows Server 2019 as a local server with standard Microsoft support until 2024.
Issues	• There is no current policy for server maintenance; therefore, there is no schedule or accountability in place to keep the server updated and secured.

	• On site, the manual backup process relies on personnel. There is no plan for catastrophic failure in place (Business Continuity and Disaster Recovery – BCDR). • The server is located in an open office, placed on a wood tray with full, unrestricted physical access, which is against best practices. • Users save data to a local drive which can be lost if an issue occurs with the local device.
Mitigation Actions	• A policy for users to save sensitive, corporate data to a network drive (OneDrive) <u>Servers:</u> **Immediate option:** • Use a third-party managed IT services firm to manage and maintain the existing server • Implement an automatic off-premises backup system • Mount the server in a secured standard rack to be protected from unauthorized physical access, which includes proper ventilation • Include a backup power solution for the server (UPS) **Recommended, long-term option:** • Migrate the SQL and File server to a cloud-based solution using Azure SQL Database and Azure Files

Potential Solutions and Costs	• Implement a BCDR (regardless of immediate or long-term approach); Refer to section 3.3.4.3 for details
	• Immediate option:
	  ○ Upgrade the on-premises server, create backup procedures and mount securely with a UPS; approximately $2500
	• Long term option:
	  ○ Migrate to a cloud system and automated backups; may be included in Azure license within M365.

3.3.4.3. Backup and Recovery Systems

General Observations	• The Township of White River backup and recovery plan consists of two Network Attached Storage (NAS) devices that are used to manually backup the file/SQL server weekly. • Computers and essential hardware do not have power backup.

Issues	• These drives are stored in a vault which can be opened by any employee. This process is not monitored or logged. • The backup solution needs to be manually completed by an employee. • A recovery strategy is required to include backup and recovery of applications.

Mitigation Actions	• A cloud backup system should be implemented to:
	  ○ reduce the risk of lost data on the Township, and
	  ○ share the liability with a cloud provider to secure and backup data.
	• Implement a BCDR solution to enable full recovery of data and/or applications for business continuity.
	• A network monitored UPS should be installed at each station and network device to reduce the impact of an outage on equipment.

Potential Solutions and Costs	• Cloud backup; May be included in Azure M365 license • BCDR solution; $198.00/ Monthly – 1TB with data and application backup and recovery • UPS installed with surge protection; approximately $500

3.4. Additional Assessments

3.4.1. Physical Security

General Observations	• The Township of White River has no centralized physical security system, nor does it have security cameras at any location.
Issues	• Every employee within the main building possesses a key that can open every door as well as a key to the vault where sensitive information is stored. • There is no monitoring or log for the keyholders or their actions.
Mitigation Actions	• A **burglary security system** should be implemented. A ULC-monitored burglary security system with protection for perimeter entries (doors and windows), dual technology motion sensors and one keypad should be installed. This will also serve as a communicator for the fire alarm system and/or the monitoring of the Automated External Defibrillator (AED), allowing for automatic notification to the fire department in the

	event of a fire/medical emergency. ATS recommends the following solution: o Vista 128BPT alarm panel with dual path communicator (GSM) o ULC approved magnetic door contacts o DT8035 motion sensor or ULC-approved similar o Alpha display keypad- • A **managed door access control system** should be implemented. A centralized access control system should be installed at main entrances and restricted areas. Using electronic credentials (cards or key fobs) will allow for easy audit of personnel as well as a centralized solution to manage access, thus removing the need for physical keys. A system capable of expansion will allow for integration of satellite offices, such as the water treatment plant and remote locations. ATS recommends: o Atrium AK22 Hybrid access control system with Web Appliance o STARPB card readers o Btag key fobs • A **surveillance system** should be implemented. A CCTV system should be installed to cover the perimeter of the building, main reception, and any critical areas. This includes an IP system with at least 5Mp (Megapixel) vandal-proof cameras and enough space to store 3 months of recording. This system will also need to be expandable to allow for the future addition of satellite offices, such as the water treatment plant and remote access if required. Recommended: this will allow for remote monitoring and corporate records in the event of an issue. o 4K 8-Channel 8MP Plug-and-Play NVR with PoE, 4 Tb storage o 5 MP Fixed Dome Network Camera.
Potential Solutions and Costs	• **Burglary security system**: approximately $4,000 installed and configured • **Access control system**: approximately $2,500 per door (depending on door type) • **CCTV (Surveillance) system**: approximately $5,500 for an 8-camera system with recorder; installed and configured

3.4.2. Phone System

General Observations	• The Township of White River is using a digital Toshiba PBX system with 4 main lines and eight extensions. • The internet, phone, fax, and debit machine are connected to the same line as the fax, which kicks off the internet transaction.
Issues	• Toshiba has discontinued this product as well as its support. Complaints about daily malfunction were common during stakeholder interviews, including dropped calls from Township citizens and incomplete call transfers. These are known issues associated with this model of Toshiba PBX phones due to their age and the fact that Toshiba no longer supports these systems. • The Township requires a reliable line for emergency services
Mitigation Actions	• Install a current, on-premises phone system that enables satellite locations as extensions to address phone issues and provide reliability for emergency services.
Potential Solutions and Costs	• New on-premises phone system - approximately $5000 including installation

3.4.3. Infrastructure Warranty Status

General Observations	• The Township of White River has no infrastructure warranties.
Issues	• Infrastructure is not protected long-term.
Mitigation Actions	• Obtain extended support from vendors for on premises hardware Or • Move to a cloud provider, which includes upgrades and long-term protection
Potential Solutions and Costs	• Manufacturer extended warranty for on premises server: starting at approximately $200 per year based on term and support level OR • Move to a cloud provider, which includes warranty and upgrades in the monthly cost ATS recommends the cloud-based solution as noted above.

3.4.4. Processes

General Observations	The assessment and discussions with Stakeholders revealed opportunities to improve in the areas of: • Accessing centralized information/data to fulfill their current roles • Accessing job training materials in one area • Having a reliable organization to contact for technology-related issues, with a defined escalation process with contractual service level agreements (SLA) • Basic end user training on city systems, software, and devices due to varying degrees of experience • Technology education of end user cyber security best practices e.g., phishing scams • Reducing manual data entry by integrating systems (e.g., manually entering tax receipts which can be received by batch EFT payments) • Standard policies that align with best practices (e.g., saving to network drives, disable USB drives etc.) • On-boarding/off-boarding employees: Honour system used to remove individuals as administrators from social media accounts. (i.e., Facebook) as well as reusing email addresses for employees.
Issues	• Impact to users if they do not understand current technology • Scalability to increase technology support to citizens, e.g., receiving online payments, etc. • Impact to city productivity • Potential data breaches if data is not secured
Mitigation Actions	• Create a centralized repository containing job-related information such as policies and training • Create and communicate policies and procedures that include eliminating the honour system for removing social media account access • Review system integration opportunities for feasibility to reduce manual work • Train end users on basic technology • Create one point of contact for technology-related issues and escalation
Potential Solutions and Costs	• Included in above assessment

3.4.5. Skill Set Gaps

General Observations	With the departure of the former resource supporting IT onsite, there is a lack of resources familiar with technology standards and best practices onsite. These gaps include supporting and maintaining onsite infrastructure (i.e., servers, computers and other devices) along with software such as M365. The lack of proper IT management puts the municipality at risk.
	• There are multiple companies to call for support
	  ○ Some helpdesk services are provided from Sudbury
	  ○ Separate companies to call for phone issues
	  ○ Email and domain issues – call vendor (Sencia)
	  ○ General lack of knowing who to call

Issues	• No centralized process for technology-related issues or management; therefore, people do not know who to contact, resulting in downtime, inefficiencies, and impact to productivity.

Mitigation Actions	• Move to a cloud-based system to reduce reliance on onsite personnel to support, maintain and backup equipment
	• Use a managed IT services firm to support users and devices
	  ○ One point of contact for users to call for help (helpdesk)
	  ○ One point of contact to monitor and manage services, maintaining compliance and best practices
	  ○ Proactive device monitoring, allowing issues to be resolved before they are visible to users

Potential Solutions and Costs	• Use a managed IT services provider to manage:
	  ○ **Remote Monitoring.** To proactively observe and resolve issues
	  ○ **User Support.** To provide rapid assistance for hardware and software related issues, basic user guidance and education, and on-going cyber-security awareness
	  ○ **Device Maintenance.** Implementation of patch and security updates
	  ○ **Reporting.** Insights into the environment to understand the Township's IT risk profile, including downtime, support, and SLA audits

3.5. Application and Other Details

3.5.1. Applications

Name	Use	Notes
Vadim – iCity	Financial ERP system designed for municipal government	Has the functionality to provide customers the ability to review their account balances online. The Township would like to enable this but requires technology updates.
Sencia	Hosted email and website domain	
M365 (Microsoft 365)	Productivity – Word, Excel, Email, Teams, PowerPoint, SharePoint	Also known as Office365
Zoom	Video conferencing	
Team Viewer	Remote access used to support IT	
Sentinel One	Server anti-malware	Installed on server only
Bitdefender	Antivirus	Installed on some computers; licence has expired

3.5.2. Social Media

3.5.2.1. Website:

- https://www.whiteriver.ca/
- Hosted by Sencia Canada.
- Hosting Provider: TBayTel.
- IP (Internet Protocol) Address: 216.211.21.166.
- Nameservers: ns2.s7host.net and ns1.s7host.net.
- Managed in-house

3.5.2.2. Facebook

- Three different Facebook pages
- Several administrators to site linked to personal accounts.
- Honour system used to remove administrators once they leave the organization

4. A/V Recommendation for Council Chambers

Considering the size and user requirements of the audio-visual system to conduct meetings in the Chambers, ATS recommends using Microsoft Teams with an HD Video Conferencing System. This includes:

- HD video conferencing with 1920 x 1080 HD resolution
- Speakerphone with Bluetooth
- Noise reduction technology
- Plug & play Simplicity
- Digital camera with pan, tilt and zoom capabilities
- Desktop computer with Microsoft Teams and a minimum 50" TV monitor (or integrated with the current projector onsite)

Microsoft Teams is standard with the Township's current M365 license and can be used as a secured method for both internal and public meetings. It also includes recording functionality.

The cost for the audio/visual system is approximately **$3,500** using the existing projector.

5. Infrastructure Upgrade Plan

To bring the Township's infrastructure up to current standards and best practices, while creating a cost-effective solid foundation for cyber security and future scalability, ATS recommends the following plan:

5.1. Modernize Hardware

i. Migrate to a hybrid cloud solution. This uses the current license and on-premises server to provide security compliance and reliability.

ii. Upgrade telephones from end of life, Toshiba phones to an updated, on-premises solution which includes continuous support and maintenance.

iii. Upgrade end user computers and devices to current standards, with SSD (approximately 6 desktops and 12 laptops). This includes outdated peripherals (monitors) and council laptops.

iv. Modernize council chambers with audio/video conferencing capabilities (refer to Section 4 for details).

v. Implement an ISP failover solution for business continuity.

vi. Implement UPS devices where recommended.

5.2. Address Physical Security Gaps

i. Resolve current server placement issues

ii. Install centralized access control at the main building

iii. Install an alarm system to monitor for burglary along with smoke, fire, and AED

iv. Install access control (key fobs) at locations with integrated, centralized management

v. Install a CCTV system (cameras) at all locations with centralized management (remote access capabilities)

5.3. Utilize M365

Fully deploy and train staff on accessing the secured Microsoft suite of applications (including Word, Excel, Power Point, Outlook, SharePoint) remotely. This includes using Teams to communicate remotely among staff members and for council to conduct Township meetings.

M365 includes Azure AD, which enables authentication to access endpoints and cloud-based applications.

5.4. Create a Centralized Data Repository

Currently, the Township eithers saves documents to the p: drive or locally on computers. ATS recommends creating a centralized repository for information that can be accessed by employees. This provides an audit trail for document management and enables collaboration on shared documents.

This can be accomplished using SharePoint, currently included in the Microsoft 365 subscription. This supports document management for remote working, as opposed to a shared p: drive.

5.5. Provide End User Basic Technology Training

As the end users demonstrated a large range of technical skills, (some very limited and others more advanced), ATS recommends providing basic end user training on devices, and M365 software. This includes tutorials for basic technology use (e.g., accessing files online), applications including Word, Excel, Outlook, PowerPoint, SharePoint, and Teams, along with an initial cyber security awareness session.

Modernizing the infrastructure will protect the Township's critical data, while enabling greater secured remote access for staff, and increased protection from cyber attacks, including ransomware.

6. Data Safety and Security Plan

Data safety and security is paramount to the Township's operations. It protects the Township and citizens' personal data. After the hardware and physical gaps are addressed in the infrastructure upgrade, ATS recommends implementing the following measures:

6.1. Strengthen Network Security

i. Implement a firewall
ii. Implement endpoint protection
iii. Implement malware protection

6.2. Implement Business Continuity and Disaster Recovery

Implement a BCDR tool to provide backup and recovery protection.

6.3. Implement Policies & Processes

Implement data access, backup, and retention policies (passwords, backups, disaster recovery etc.) Communicate the policies to end users and store on a centralized, internal site (i.e., SharePoint).

6.4. Implement a Cyber Security Education Program

Provide end users with ongoing cyber security awareness training and documentation, including potential phishing emails with click statistics and current threats.

6.5. Hire a 3rd Party Managed IT Services Provider

A managed IT Services provider will manage the implementation of network security along with ongoing monitoring, maintenance, and support. They also act as the Township's helpdesk to provide remote support to employees where needed and emergency support services. Additionally, some managed service providers provide cyber security awareness training.

6.6. Acquire Technology Leadership

Use a technology lead for overseeing critical technology decisions, policies and to ensure alignment with the Township's strategic direction. This can be achieved using a virtual CIO that can work part time with the Township to lead technology resources, roadmap, and strategy.

7. Estimated Implementation Timeline and Cost

7.1. Timeline

Based on ATS' experience executing these deliverables, the estimated, high-level timeline to implement the recommendations is approximately three months.

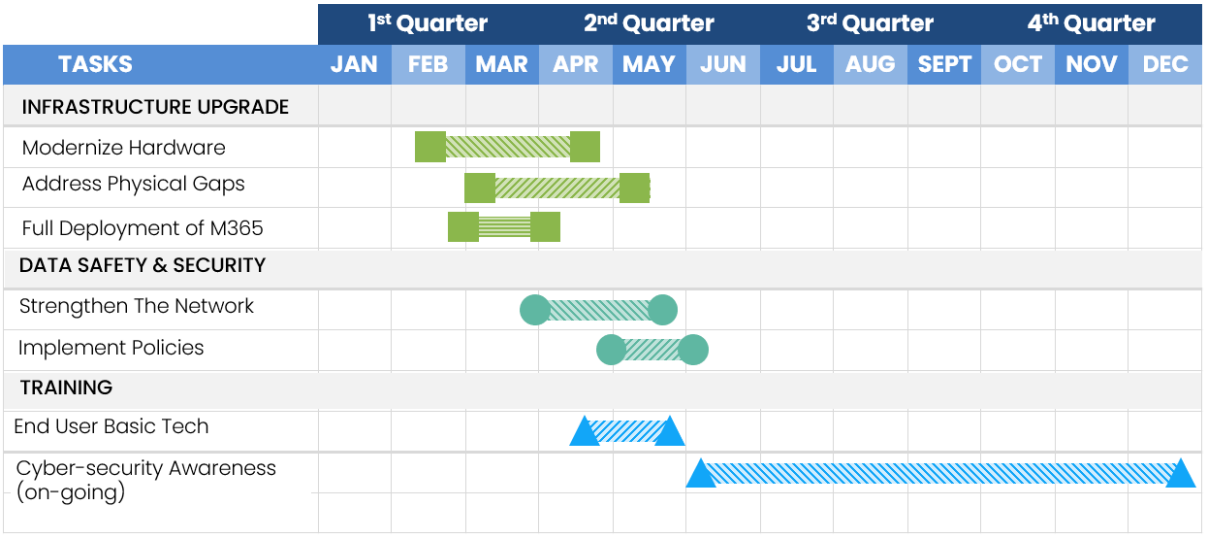

Figure 14 Estimated Implementation Timeline

Assumptions include resource availability and executing tasks in parallel.

7.2. Cost

To implement the critical recommendations noted in this assessment, the estimated one-time cost with one year support is approximately **$149,878**.

Monthly costs after the first year are approximately **$3,500** which includes ongoing managed IT services support.

8. Appendix: ATS Service Offerings

Our Services

MANAGED IT SERVICES

- Network Design, Installation and Support
- Infrastructure Assessment
- Service Delivery
- Cyber Security Assessment
- Data Protection
- Business Continuity Services
- Wi-Fi Design and Monitoring
- IT Standards & Policy Design
- Monitoring and Response
- Network Assessment
- Office 365 Implementation
- Perimeter Security
- Endpoint Protection
- Disaster Recovery Solution
- Desktop support
- Work From Home (WFH)

TELECOMMUNICATION SERVICES

- Cloud Commercial Phone Systems
  - ACO - Avaya Cloud Office by Ring Central
- On Premise Commercial Phone Systems
- SIP - Session Internet Protocol
- VoIP - Voice Over Internet Protocol

INFRASTRUCTURE

- Data Center Design
- Rack and Stack
- Structure Cabling Installation
- Cloud Assessment

PHYSICAL SECURITY

- Intrusion Detection(Alarm Systems)
- Access Control
- Panic Buttons
- CCTV-Surveillance Systems
- Nurse Call Systems
- Fire Panel Monitoring & Installation

PROFESSIONAL SERVICES

- Project Management
- Virtual CIO

BELL PRODUCTS AND SERVICES

- High Speed Internet Connectivity
- Entertainment Requirements
- Remote Internet Connectivity
- Mobile Devices

705-759-8999 | 270 Bruce Street, Sault Ste. Marie | sales@atstechnology.ca | www.atstechnology.ca