Who's providing advice and support to Pacific Island countries?

We are. LGNZ.

PacificTA

LOCAL GOVERNMENT NEW ZEALAND TECHNICAL ASSISTANCE FACILITY

Port Vila Municipal Council

IT Management

16 – 21 September 2018

This report has been prepared by Aaron Williams, IT Support Engineer with Tararua District Council, following a visit to Port Vila in September 2018.

This report is the opinion of Aaron Williams. It should be used in conjunction with other reports and information and does not necessarily reflect the views of Local Government New Zealand, Tararua District Council or the Ministry of Foreign Affairs and Trade.

NEW ZEALAND
FOREIGN AFFAIRS & TRADE
Aid Programme

PacificTA is funded by New Zealand Foreign Affairs and Trade Aid Programme

Table of Contents

Executive Summary 4

IT Summary 5

- **Assessment Goal** 5
- **Assessment Procedure and Scope** 5
- **Assessment Summary** 6

Assessment Detail 7

- **Server/NAS** 7
- **Server Physical Environment** 7
- **Firewall/Router** 7
- **Backups** 7
- **Antivirus** 8
- **Internet** 8
- **Wireless** 8
- **Workstations** 9
- **Email** 9
- **Licensing** 9
- **Switching/Cabling** 9
- **Policies and Procedures** 10

Action Plan 11

Executive Summary

The Port Vila Municipal Council (PVMC) 100 Day Plan identifies the need to update the accounting system, computerise invoices and receipts and the HR management system. An upgrade to IT is critical to support these changes.

Upgrading IT will also support:

- Systems security to prevent external attacks e.g. the crypto locker virus
- Improvements in staff efficiency and future growth in council employees
- Staff training opportunities through access to on line tutorials e.g. MYOB and IT
- Back-up systems to meet audit requirements
- Online Communications e.g. Microsoft Skype
- Software updates and access to online applications
- Improved web site functionality, e.g. PVMC application forms are available on the web
- Enhanced disaster recovery through back-ups

A number of actions are recommended including an upgrade of the server and back-up systems to support audit requirements and to protect council data in disaster.

The Tararua District council has provided a firewall which was installed to improve PVMCs IT security. This does not protect PVMC from email attacks and other application penetration via attachments and downloads by users and it is recommended that PVMC install an additional license to enable the integrated antivirus in the Firewall.

Increasing the internet speed is recommended to enable key software such as MYOB to be upgraded. This will also enable PVMC staff to access on-line tutorials in MYOB. The MYOB license will need to be updated.

IT Summary

The Port Vila Municipal Council (PVMC) 100 Day Plan identifies the need to update the accounting system, computerise invoices and receipts and the HR management system. An upgrade to IT is critical to support these changes and update the security of council files and hardware.

The IT environment that supports PVMC comprises of five units (including finance, executive and planning) in the central council building and two external offices (wardens and works division). The initial IT infrastructure was configured by SPIM in 2015 for 25 users.

There is a fibre enabled router connection that provides all Internet traffic going in and out. There are two Windows servers in place, supported by various switches and a LTE Router. There are a mix of Windows workstations. Email is held on the local internal server (not cloud based) using 3rd party software Kerio Mail and backups are stored locally. These conditions are typical of a small to medium business but would not be used in councils due to potential security risks and reduced functionality.

The IT unit have suggested that Council documents such as planning and other applications are made available online e.g. council agendas and minutes, infringement fees and application forms.

Assessment Goal

PVMC is currently auditing its IT environment to ensure optimal support to achieve Council goals. The Councils IT and IT Assessment goals include:

- Performance & Stability – IT infrastructure and policies to minimise disruption.
- Risk Assessment – Review IT Systems and procedures for current opportunities for improvement as well as facilitating future growth.
- Software system and applications – review licensing and functionality.
- Staff Capability – Review Staff Training requirements.

Assessment Procedure and Scope

The assessment included reviewing network tools, PVMC documentation, and direct observation to identify risks and opportunities for improvement in the IT environment. A traffic light system flags observations from the Assessment as green, yellow, and red.

GREEN	From no risk to mild risk – no immediate issues and/or minimal consequences
YELLOW	From mild risk to medium risk – will require attention in the next 3 months and/or not aligned with best practices.
RED	From medium risk to urgent risk – imminent issue and/or serious consequences

Throughout each of the 12 areas reviewed in the Assessment, the 3 core pillars approach was used, called SMB “Secure, Manage, Backup” IT:

- Secure IT – Can it be secured and how do you know it is secured?
- Manage IT – Can it be managed and how do you know it is managed?
- Back IT up – Can it be backed up and how do you know it is backed up?

The scope of this assessment was for PVMC internal IT and public website.

The term workstation refers to desktops, laptops and tablets.

Assessment Summary

This IT Assessment is to provide suggestions on how the PVMC IT environment could be enhanced to better support Council goals. As recognised by the Council IT team, the current IT infrastructure, support model, processes, and procedures can be improved to support current and future Council needs. There are also some processes and procedures that are not documented such as new staff training and IT set up (induction/on boarding processes), disaster recovery plans.

A summary of the areas reviewed in the assessment 17-21 September, and their colour coded flags are listed below:

Flag	Area reviewed	Summary assessment
RED	Server/NAS	No NAS (network attached storage) but it is quoted for. Server Setup is YELLOW.
YELLOW	Server Physical Environment	Minimal Hardware and no Redundancy present. 2 x Physical machines running Hyper V Server.
RED	Firewall / Router	Non-existent
RED	Backups	Some discrepancies with what needs to be backed up and how often.
RED	Antivirus	Not licenced or updated. Conflicting installs of AV on servers.
YELLOW	Internet	Fibre, 2 MB connection.
YELLOW	Wireless	Is located in server with limited range (5 metre radius).
YELLOW	Workstations	All workstations are not consistent and are running windows 7 with some windows 8.
YELLOW	EMAIL	Locally installed 3rd party software for emails (Kerio Mail) Expired Certificate.
RED	Licensing	Fully up to date and centralized repository is not present. Some unlicensed Servers.
YELLOW	Switching/cabling	Unmanaged switches present in some open workspaces and some health and safety issues with cables in walk spaces.
RED	Policies and Procedures	Some best practices documentation and procedures are not in place, such as: IT induction /"on boarding" process, disaster recovery plan, hardware and software lifecycle plan, network use policy and Network diagrams.

The following pages provides detail on each of the areas listed above with actions for improving the PVMC IT environment. Tararua District Council will provide estimates for remediation and optimisation based on the outcome of discussions for the report.

LGNZ and Tararua District Council thank PVMC for allowing us to perform this IT Assessment. We trust that it will be valuable to you as you decide how to ensure that IT supports your Council goals.

Assessment Detail

Server/NAS

RED: There are currently two physical Windows servers running Hyper-V with 2 VM's on each. Some configuration needs to be addressed on the Hyper-V level and in the VM's like time sync and DNS, DHCP, and Active directory. One server has been abandoned and taken off the network due to age and because it was infected with crypto locker virus. Backup processes are not currently sufficient (see Backups above).

Action - It is recommended that the recently quoted New Server be purchased and installed, along with the new licensing and certificates so that it is functioning in a secure manner. A NAS hard drive is necessary for backups of the new and or old servers.

Server Physical Environment

YELLOW: Air conditioning in the Server/IT room is adequate, however the network cabinet and surrounding need to be tidied up for health and safety purposes and general ease of management. There is no temperature monitoring and alerting in place. Access to the Cabinet should be restricted and monitored.

Action - It is recommended that all IT components in the Cabinet be powered by the existing Uninterrupted Power Supply. However, the existing UPS is insufficient and is in need of upgrading.

Action – Increase security of Server cabinet. Options could include:

- Webcam installation
- Security Cage
- Restricting access to IT department

Firewall/Router

RED: Firewall device is was non-existent.

Action – Implementation of a donated firewall has been completed on Wednesday the 19th September 2018. This has been configured to protect some of the network behind it.

This does not protect PVMC from Email attacks and other application penetration via attachments and downloads by Users without an additional license to enable the integrated antivirus in the Firewall.

Action - It is recommended that Council purchase the extra license to enable email protection.

Backups

RED: Backups consist of an unlicensed version of Veeam Backup System. Backup is completed 2 times per week to an external USB drive and is not stored offsite. Backup of data is not consistent and needs a thorough audit of backup. Just because a backup completes successfully does not mean that all required protected data was backed up.

Action – Confirm back-ups configuration meets Council expectations.

Action - It is also recommended that routine restores are tested at least every six months to confirm backups are working correctly.

Action – Configure a form of managed local backup. Develop a spreadsheet to log backup success and failure for audit purposes:

- Full backups to a NAS hard drive should be daily onsite, scheduled to automatically run each night
- A further daily copy should be made onto a portable hard drive and taken offsite daily (two portable hard drives swapped in the morning each day), until such time as the NAS can be located offsite – see below*.
- One hard drive each should be retained for each week of a month (4 weekly rotation)
- A full monthly copy should be kept for each month of the year (12 monthly rotation), and be retained in a safe offsite
- An annual copy should be securely retained and kept offsite for 7 years.

* The NAS could be synced and housed in a Datacentre once the internet service speed has been increased to ~20mbits/s. This would need the internet connection to be upgraded from the current 2 mbits/s.

Antivirus

RED: There is a current mismatch of free and unlicensed Antivirus software throughout the servers and workstation PC's. Management and reporting of antivirus policies are only effective if there is a consistent centrally managed system in place. Antivirus can be turned off or even uninstalled while in its current state in the [Company] network.

Action - Migrate to a more effective centrally managed antivirus solution to keep up with remote users and laptop users when not on the local network and to easily centrally manage the licensing and policies pushed to the machines and servers. Suggest ESET Antivirus administration centre with licenses for File Server and endpoint for workstations.

Internet

RED: The current internet connection is failing in performance for council staff to work efficiently on the web. After testing and investigation, it was found that the current connection is running at 2mbits/s. This will not allow for offsite backup sync or updates of current critical business software like MYOB.

Action – Upgrade internet fibre connection to minimum of 4mbits/s but preferably 10-20mbits/s, subject to cost.

It is essential to have the higher speed to efficiently keep software licensing current and should cloud based software be used.

In future, a "tunnel" secure virtual private network (VPN) could be installed to connect the Council network to external provider, such as if PVMC chooses to follow the advice of MIA to consider using their financial system "Smart Stream".

Wireless

YELLOW: The main fibre router is the Wi-Fi device (ZTE router). This is in the IT server room and is not sufficient for use throughout the building. This device is only giving a radius of 5 meters which only reaches through to the Accounts office.

Action - It is recommended that a three pack of Ubiquity Unifi mesh Wi-Fi long range devices be implemented throughout the building with central management software installed and configured. This will increase functionality to mobile and other devices throughout the buildings.

Workstations

YELLOW: Currently all workstations are on Windows 7 and it will no longer be supported by Microsoft in 2019.

A domain environment is currently configured to manage workstations. However, not all workstations are connected to the domain pvmcvanuatu.local.

Furthermore, security and accounts are not configured correctly, or at all. It is recommended that all machines in their current state be updated to the latest service pack and connected to the domain for security purposes.

Action - It is recommended that all workstations be upgraded to Windows 10.

Email

YELLOW: Email consists of a 3rd party POP/IMAP with an active sync client/add-in for mail clients. This is fine for the use of PVMC however the Mail Certificate is not currently valid and this will cause issues with mail clients and emails being blocked by other recipients.

Action - Update the certificate and check email configuration.

Office 365 Email and Office can be implemented after a planning process has been completed and an evaluation of the scope required.

Licensing

YELLOW: There is no current system in place to track or monitor what applications are installed on the network. The current repository or list of software does not appear to exist.

Action - Implement an asset tracking system with capability to perform a licensing and asset audit to confirm licensing obligations are met and asset replacement is controlled.

Action – Generate a single document or location to track all licensing information such as license keys, costs, and dates.

Switching/Cabling

YELLOW: Cabling needs some care and is possibly a health and safety risk due to being untidy and on the floor in walkway areas between desks.

Cables are also aged and brittle.

Switches are in each room and are at a suitable 1 Gigabit speed. The main rack switch is a Cisco 18 port Gigabit switch connecting the rooms to the servers and router and is fit for purpose.

Action - Cables should be tidied with cable ties and cable management systems. The network switch is suitable for the purposes of current Council staffing levels

Policies and Procedures

RED: Device inventory is not kept and updated. A password policy is not in place on the domain. There is not an employee off boarding departure procedure in place.

Action - It is recommended that this document be reviewed and updated to consider high level departures with total system access. There is also no standard Employee “Induction/On boarding” or Exit procedure on file. There is no device lifecycle policy in place. Generically a 5 year lifecycle is recommended for infrastructure devices and in some cases 3-5 year lifecycles for end user devices due to the rate of change.

Action – Introduce best practices policies and documentation as noted, and customize for PVMC to standardize and minimize IT and business risk.

Action Plan

Area	Flag	Action	Associated Hardware/Labour	Associated Costs	Time Frame
Server/NAS	RED	Renew Server OS licenses and install NAS for local Backups	Installed by IT company from Quoted and purchased Hardware	VT1.6m-1.7m, subject to quote Plus staff time	6-8 weeks from order
Server Physical Environment	YELLOW	Tidy cables and Cabinet	Performed by IT staff with possible purchase of new cable replacements.	Minimal costs at the discretion of IT department	8 hours
	YELLOW	Determine IT closet access and procure lockable cage	IT staff to tidy up cables behind cabinet and move cabinet back to wall and secure the door with key. Replace old cables	Minimal cost to department	2-4 hours
	YELLOW	Install webcams to monitor IT closets and start saving video to hard drive.	Highly recommended. Necessary	VT 40,000 -60,000	4-8 hours
Firewall/Router	GREEN	Increase firewall memory and upgrade firmware	Configured and installed by Aaron Williams; Load mail license	Donated by Tararua District Council NZ. License mail security VT 17,500 p.a.	5 hours +8 hours staff time
	GREEN	Perform penetration test.	Can be completed by IT staff but not necessary	Staff time	1 hour
Backups	RED	Audit backup configuration.	Configuration of backups by IT staff	Staff time	2 hours
	YELLOW	Investigate offsite backup at Government datacentre.	Investigated by IT staff and agreed by Town Clark	Staff time	
	RED	Confirm Backup Model.	Rotate use of portable hard drives: Daily,	VT 130,000 (4 weekly +12 monthly = 16x	

			Weekly full, Monthly full and Yearly full. Secure offsite (safe?)	1TB portable hard drives)	
	RED	Test and confirm restore data.	Restore of Backup from local and offsite on a Monthly bases.	Staff time	2 hours every 6 months
Antivirus	RED	Migrate to central managed solution. Load Firewall Software	Work to be performed by IT company and IT Staff from quoted and purchased Software	VT 95,004 ex VAT Add Firewall Software ~ <22,000 VT p.a.	8 – 12 hours
Internet	RED	Increase internet speed	Upgrade internet fibre connection to 20mbits/s, subject to cost	VT 140,000 ex VAT Year 1; Reassess to increase Year 2, 2020 budget to ~280,000 VT	Change over performed by TVL
Wireless	Yellow	Increase Wi-Fi Capacity throughout the office.	Install a pack of three Wi-Fi Access Points for seamless coverage upstairs and downstairs in the council building	VT 53913 ex VAT	4 – 6 hours
Workstations	Yellow	Upgrade the OS for all workstations to Windows 10 over the next 6 months	This could be done gradually over the next 6 months	Per license per machine.	30 – 40 hours
Email	Yellow	Install Certificate for Mail	Can be purchased and installed by IT company performing upgrades.	VT 17,896 Includes upgrade of mail system and 1 year support	2 – 4 hours
Licensing	RED	Implement asset tracking.	Performed by IT staff	Staff time	4 – 8 hours
	YELLOW	Modify document and/or shared tracking	Performed by IT staff with consultation from other.	Staff time	8 hours

		workspace for better structure and ease of security implementation	Management staff time to agree configuration of folder structure.		
Switching / cabling	YELLOW	Cables throughout the office should be tidied with cable ties and cable management systems	Performed by IT staff	VT 36,000	8 weeks from order
Policies and Procedures	YELLOW	Generate best practices policies and documentation.	Performed by IT staff	Staff time	Hours will be continual to create and keep up to date
	RED	Implement hard drive redundancy.	As part of NAS and server setup	As above	6-8 weeks from order
	YELLOW	Migrate Virtual Servers from Old to New hardware	6-8 weeks from order	6-8 weeks from order	6-8 weeks from order