020/OCM/17

AMMENDMENT TO SENQU MUNICIPALITY INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICIES

PURPOSE

To amend Senqu Municipality's Information Technology (ICT) Security Policies that was adopted by Council on the 30th of June 2016.

BACKGROUND

The ICT Security Policies have been reviewed and amended to be compliant with the Senqu Organisational environment as well as improved technology.

REQUIRED CHANGES

Patch Management

- Remove: Workstations and servers owned by the Municipality must have up-to-date (as defined by Global Systems Office's minimum baseline standards) operating system security patches installed to protect the asset from known vulnerabilities.
- Replace with: Workstations and servers owned by the Municipality must have up-to-date (as defined by this policy) operating system security patches installed to protect the asset from known vulnerabilities.

- Insert: Patches are not flawless and sometimes cause more harm than good. Harmful patches are usually withdrawn or rectified within a week of release. Patches will be downloaded to the WSUS Server daily, but held back for at least a week and then released, after being checked by the ICT Manager, to upload to other servers and workstations if it was not withdrawn or if a rectification did not come through during the past week.

- Remove: Servers must comply with the minimum baseline requirements that have been approved by the Global Security Office.
- Replace with: Servers must comply with the minimum baseline requirements that have been approved by the Specifications Committee.

- Remove: Users will be informed by means of email of monthly and emergency patch management deployments.

- The IT Administrator is required to compile and maintain reporting metrics that summarize the outcome of each patching cycle. These reports shall be used to evaluate the current patching levels of all systems and to assess the current level of risk. These reports shall be made available to Management and Internal Audit upon request. For a municipality of our size, this is just about impossible as you need a test environment and a person dedicated to testing, evaluating and reporting and you still have no guarantee that nothing was missed.

- Replace with: The IT Administrator is required to keep evidence of patches implemented as well as implemented patches that caused problems and make it available to Management and Internal Audit on request.

- Remove: Server Specs must contain the operating system level, service pack, hotfix, and patch level. Hot fixes and patch levels happen all the time and any time and cannot be built into specs. Hotfixes and patches are loaded from the internet when the server is set-up.
- Replace with: Server Specs must contain the operating system level and service pack.

Security Training

- Remove: seminar
- Replace with: in-house training

Computer Virus Detection

Remove:

- Every virus that is not automatically cleaned by the virus protection software constitutes a security incident and must be reported to the Anti-Virus Help Desk.
- Replace with: Every virus that is not automatically cleaned by the virus protection software is put into quarantine and automatically uploaded to Antivirus Labs for deconstruction and patch release.

Network Configuration

Remove:

- ❖ Packet sniffers. We do not have such a high level next generation firewall. It is expensive.
- ❖ Intrusion Detection. Intrusion Detection no – very high level but requires next generation firewall and dedicated highly trained network security staff to man 24/7.

Electronic Mail

- Remove: The Municipality does not maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up automatically on every user's workstation.
- Replace with: The Municipality may maintain central or distributed electronic mail archives of all electronic mail sent or received. Electronic mail is normally backed up automatically on every user's workstation.

FINANCIAL IMPLICATIONS

None

1

LEGAL IMPLICATIONS

None

*** Attached as **Annexure "G" page 512-594** is the ICT Security Policies with proposed amendments.

CREDIBILITY

The report was submitted by Manager IT and was verified by CFO

RESOLUTIONS

(a) Council noted the amendments and approved the Information Communication Technology Security Policies.