SECURITY MANAGEMENT

Date of adoption: 23 May 2017
Council resolves to adopt the under-mentioned revised policy as the Information Technology Policy of the DR BEYERS NAUDE LOCAL Municipality

TABLE OF CONTENTS

1. SCOPE OF POLICY

The **BNLM** ICT Security Policy is applicable to all employees within the municipality, third parties and stakeholders utilising the municipality's ICT infrastructure and resources in order to fulfil the municipality's goals and objectives

2. PURPOSE

The purpose of the ICT Security Policy is to ensure the effective protection and proper usage of the computer systems and its peripherals within the municipality. Each employee is responsible for the security and protection of electronic information resources over which he or she controls. Resources to be protected include, but not limited to networks, computers, software, removable media and data. The physical and logical integrity of these resources must be protected against threats such as viruses, sabotage, unauthorised intrusions, and malicious misuse or in-adverted compromise.

3. RESPONSIBILITIES

3.1 Senior Manager: Finance

3.1.1 The Senior Manager: Finance is responsible for overseeing the development and implementation of the Municipality's ICT Security Policy.

3.1.2 In consultation with the Systems Administrator, the Senior Manager: Finance shall recommend all ICT improvements of the municipality to the Director: Finance and Corporate Services. Where necessary, a report with recommendations will be submitted to Council.

3.1.3 Ensure that all ICT service providers undergo the necessary security procedures before providing services to the municipality i.e. assessing the credibility and competence of the Service Provider.

3.1.4 Ensure that Risk Management Policy of the municipality is adhered to in the ICT Unit. Identify mitigating actions to reduce the ICT risks of the municipality to an acceptable level and make recommendations where necessary.

3.2 Systems Administrator

3.2.1 Responsible for overseeing the implementation of the ICT Security Policy.

3.2.2 Maintain and manage relationships with stakeholders and Service Providers by ensuring that all Service Level Agreements entered into are monitored in terms and conditions therein.

3.2.3 Monitor and ensure compliance with relevant ICT Regulatory Framework.

3.2.4 Ensure that all ICT physical security breaches are reported immediately to the Senior Manager: Finance.

3.2.5 Responsible for physical protection of all ICT assets of the municipality.

3.2.6 In conjunction with Asset Management, ensure that employees are provided with approval to move any ICT assets, other than mobile devices.

3.2.7 Ensure that the municipality's environment is secured from any internal and external threats.

3.3 Internal Audit

3.3.1 Internal Audit shall audit all ICT Compliance within the municipality

3.3.2 Assist ICT Unit in ensuring that recommendations provided from the audit findings are implemented correctly.

4. THIRD PARTIES AND CONTRACTORS

4.1 All ICT Service Providers shall be screened before providing services to the municipality to ensure credibility of the service provider.

4.2 Sign a non-disclosure of classified information.

4.3 A Service Level Agreement must be signed between the municipality and Service Provider before providing any ICT services.

4.4 A Service Provider shall not be provided with any logical access to any critical information systems; access will be provided only with approved authorisation from the Senior Manager: Finance.

5. ASSET MANAGEMENT

5.1 All ICT equipment shall be recorded in the Fixed Asset Register and allocated an asset number.

5.2 The ICT asset register shall have at least the following descriptive fields:

Asset number, asset owner, location of the asset, category of asset, date of acquisition, asset description and value of the asset.

6. SERVER AND NETWORK ROOM

6.1.1 Servers shall be located in a secure server room that is accessed only by authorised ICT employees.

6.1.2 Service Providers shall not access server rooms without being accompanied by an ICT Unit employee.

7. PATCH MANAGEMENT

7.1 Patch Management is the responsibility of the Systems Administrator.

7.2 The Systems Administrator shall identify patch management resources to update the servers and workstations of the municipality.

7.3 Workstations and servers owned by the municipality must have up-to-date operating system security patches installed to protect the asset from known vulnerabilities. This includes all laptops, desktops, and servers owned and managed by the municipality.

7.4 Desktops and laptops must have automatic updates enabled for operating system patches. This must be the default configuration for all workstations and any exception to the policy must be documented in the Patch Management Log Book.

7.5 Servers must comply with the minimum baseline requirements. These minimum baseline requirements define the default operating system level, service pack, hotfix, and patch level required to ensure the security of the municipality asset and the data that resides on the system. Refer to the server security baseline in Section 17.

7.6 Patches will be tested for a maximum period of 14 days in a test environment prior to deployment into the live environment.

8. DESKTOP SECURITY

8.1.1 All desktops provided to employees shall be allocated in accordance with the employee's job description.

8.1.2 Employees shall be given Standard User Access to the desktop operating systems.

8.1.3 Employees shall ensure that they only utilise the equipment for official purposes.

8.1.4 Employees shall only have logical access to their desktop computer.

8.1.5 No employees, except ICT Unit employees are allowed to disassemble or perform repairs to any ICT equipment.

8.1.6 No desktop computers shall be removed from an employee's office without the authorisation of the Systems Administrator and Asset Management.

9. MOBILE DEVICES

Mobile devices herein refer to laptops and tablets.

9.1.1 Municipal mobile devices shall be issued to employees in accordance with the Asset Management Policy

9.1.2 All employees issued with municipal laptops must ensure that they are also provided with security cables.

9.1.3 It is the employee's responsibility to ensure that the laptop is secured at all times.

10. REMOVABLE DEVICES

Removable devices herein refers to USB Flash Drives, Compact and DVD discs, external Hard-drive and any other removable media storage devices.

10.1 Removable devices shall be issued to employees in accordance with the Asset Management Policy.

10.2 Any loss of removable devices allocated to an employee must be reported in writing to the ICT Unit within 48 hours.

11. NETWORK SECURITY

11.1 Only municipal desktops and mobile devices shall be connected to the municipal network.

12. REMOTE ACCESS

12.1 Remote access to operational systems is prohibited i.e. PSM Logic, Appx.

12.2 Only the Systems Administrator and the IT Technician are permitted to have remote access via Virtual Private Network (VPN).

12.3 Remote access will only be granted to an employee in exceptional circumstances with the approval of the Director: Finance and Corporate Services.

13. INTERNET AND EMAIL

13.1 Internet and Email Security Management forms part of the ICT Code of Conduct, which must be signed by all users of Municipal Internet and Email facilities.

14. MALICIOUS SOFTWARE

14.1 Employees are prohibited from installing unauthorised software.

14.2 Malicious software (Virus, Trojans, Worms and Spyware) identified by an employee must be reported immediately to the Systems Administrator or the IT Technician. The reporting of the incident is as follows:

- Contacting the IT helpdesk to report the incident
- IT technician shall assist the user to remove the Malicious software
- Systems Administrator must ensure that the Antivirus installed on all is setup to scan desktops and servers daily.

14.3 ESET Endpoint Protection is currently in use and user computers are updated daily. Any computer, laptop or other device that is found to be infected with a virus must be attended to immediately and quarantined.

14.4 A record will be kept of all types of malicious software encountered.

15. FIREWALL AND ANTIVIRUS

15.1 It is the responsibility of the Systems Administrator to ensure the effective implementation of firewall and antivirus management for the municipality.

15.2 The Systems Administrator is responsible for ensuring that the latest version of antivirus software is installed and signature database is up-to- date.

15.3 Users of mobile devices should ensure that computers are plugged into the Municipal network at least once a week for antivirus updates.

15.4 Employees are prohibited from disabling or interfering with the virus scanning software.

16. INCIDENT MANAGEMENT

16.1 All the municipal ICT incidents must be reported to the ICT Department

16.2 ICT incidents shall be prioritised according to the risk and impact they have on the municipal network and critical systems.

16.3 Spiceworks shall be the tool used for logging ICT incidents.

17. THE SERVER SECURITY BASELINE

17.1 Basic Security Step:

- Plan the installation and deployment of the operating system and other components for the server.
- Install, configure, and secure the underlying Operating System.
- Install, configure, and secure the server software.
- For servers that host content, such as Web servers (Web pages), File Servers, and Active directory servers, ensure that the content is properly secured. This is highly dependent on the type of server and the type of content, so it is outside the scope of this publication to provide recommendations for content security.
- Employ appropriate network protection mechanisms like firewall, packet filtering router, and proxy.
- Choosing the mechanisms for a particular situation depends on several factors, including the location of the server's clients (Internet, internal, and remote access), the location of the server on the network, the types of services offered by the server, and the types of threats against the server.
- Employ secure administration and maintenance processes, including application of patches and upgrades, monitoring of logs, backups of data and OS, and periodic security testing**.**

17.2 The following items are important to consider, and will make the process of employing security controls more efficient:

- Identify the purpose of the server.
- Identify the network services and protocols that will be provided on the server examples include **HTTP, FTP, SMTP, NFS, and TCP/IP**.

- Identify any network service software, both client and server to be installed on the server and any other support servers.
- Identify the users or categories of users of the server and any support hosts.
- Determine the privileges that each category of user will have on the server and support hosts.
- Determine how the server will be managed (locally, remotely from the internal network, remotely from external networks).
- Decide if and how users will be authenticated and how authentication data will be protected.
- Determine how appropriate access to information resources will be enforced.
- Determine which server applications meet the organization's requirements.
- Consider servers that may offer greater security, even though with less functionality in some instances.

17.3 SERVER ROOM PHYSICAL LOCATION CONSIDERATIONS

When planning for this location, the following were considered:

- Appropriate physical security protection mechanisms for the server and its networking components, including locks, card reader access, security guards, and physical intrusion detection systems like motion sensors, cameras).
- Appropriate environmental controls so that the necessary humidity and temperature are maintained, and the possible need for redundant controls.
- Backup power sources and how long power can be provided.
- Appropriate fire containment equipment that will minimize damage to equipment that would not otherwise be impacted by the fire.
- Redundant network connections and redundant data center locations for high availability systems.
- Protection from potential natural disasters that may exist in the server location.

17.4 STRENGTHENING AND SECURELY CONFIGURING THE OPERATING

SYSTEMS

Remove or disable unnecessary services, applications, and network protocols

The following provide some examples of what services, applications, and protocols that can be removed / disabled if they are not being utilized:

- File printer sharing services (Windows Network Basic Input / Output System [NetBIOS] Network File System [NFS], FTP.
- Wireless networking services.
- Remote control, remote access programs, particularly those that do not strongly encrypt their communications example Telnet.
- Directory services like Lightweight Directory Access Protocol [LDAP], Network Information System [NIS]).

17.5 Enforcement

Implementation and enforcement of this policy is ultimately the responsibility of System Administrator as well as Employees of BNLM. Information Security and Internal Audit may conduct random assessments to ensure compliance with policy without notice. Any system found in violation of this policy shall require immediate corrective action. Violations shall be noted in the BNLM issue tracking system and support teams shall be dispatched to remediate the issue. Repeated failures to follow policy may lead to disciplinary action.

18. GENERAL

18.1 All employees provided with ICT equipment must ensure that the ICT equipment is protected from damage and theft at all times.

18.2 Any damage to or theft of ICT equipment must be reported writing to Asset Management within 48 hours.

18.3 Employees not reporting any damage or theft of allocated ICT equipment shall bear the responsibility and the losses recovered from them. This shall be done in compliance with the Asset Management Policy.

19. REVIEW

19.1 This policy shall be reviewed at least annually.

Annexure A: ICT Asset Movement Form

Section 1: Requesting Employee Information		
Department:		
Name & Surname	**Telephone No**	**Email**
Reason:		

Section 2: Asset Information		
Asset No	**Current Location**	**Destination**

Section 3: Authorization			
	Initial & Surname	**Signature**	**Date**
Department Head:			
ICT Unit Employee			
Asset Management:			