INFORMATION TECHNOLOGY STRATEGY POLICY FOR THE JOHN TAOLO GAETSEWE DISTRICT MUNICIPALITY

Policy Resolution Number:6.4.29/05/2018	**Approved Date:29 May 2018**
Effective Date: July 2018	**Review Date: As and when required**

SIGNATURE OF THE MUNICIPAL MANAGER

SIGNATURE OF THE SPEAKER

Ms P [illegible]

Speaker

PASSWORD POLICY

A strong password must have the following characteristics:

1.1.1 Lower case characters

1.1.2 Upper case characters

1.1.3 Numbers

1.1.4 Punctuations

1.1.5 "Special" characters (e.g. @,#&%$()_<>~+={}[];/',)

1.2 Contain at least fifteen alphanumeric characters.

1.3 Weak password has the following characteristics and must be avoided:

1.3.1 The password contains less than fifteen characters

1.3.2 The password is a word found in a dictionary (English or Foreign)

1.3.4 The password word is a common usage such as:

- Name of family , pets, friends, co-worker, fantasy characters, etc,
- Computer terms and names, commands, sites, companies, hardware, software,
- The words "John Taolo Gaetsewe", "jtgdm", "jtg", or any derivation.
- Birthdays and other personal information such as address and phone numbers
- Word or numbers like aaabbb, qwerty, zyxwuvts, 123321, etc.
- Any of the above spelled backwards.

INTERNET POLICY

- Use of the Internet for email, web searches, authorised municipal transactions, Web Development and research is permitted only for Municipal business use only by employees of the municipality.
- The use of the Internet will support the municipal objectives.
- Users will be granted authorization to use the Internet and will receive required training prior to being given a USER ID and PASSWORD.
- Users will acknowledge that they have received training, read and understood the Internet, email, and related policies governing appropriate use by signing the related acknowledgement forms.
- Access to the Internet will be through the Firewall.
- All files downloaded from the Internet will be scanned for viruses at the firewall and on the user's desktops, laptops and any other computer devices.
- Users are advised that the frequency of new viruses is high and antivirus software may not contain definitions to clean the most recent viruses. For this reason, downloading of files from unknown sources is prohibited. The users assume full responsibility for any viruses entering the John Taolo Gaetsewe District Municipality`s network through the downloading of the viruses of files from the Internet and the use of USBs'.
- Use of the Internet resources for personal business, email, Web-surfing, and the development of personal Web sites is strictly prohibited.

- All users will present professionalism when using the Internet.
- Confidential and sensitive information will not be transmitted over a public network, such as the Internet, unless approved authentication and encryption mechanisms have been employed.
- Web based applications that support marketing will establish mechanism for authenticating the sources and destinations of transmission. No client or potential client information of the Municipality will be transmitted over the Internet without the express permission or approved authentication and encryption mechanism in place.
- Use of the Internet for discussion groups for business purposes will represent responses with the following banner" **The views expressed in the message are my own and do not represent that of my employer."**
- Users will report unusual activities or suspect breaches of security to the Information Security Officer.

ACCOUNT MANAGEMENT POLICY

- All accounts created must have an associated request and approval that is appropriate for the system or service.
- All users must sign the Network Access Request Form before access is given to an account.
- All accounts must be uniquely identifiable using the assigned user name.
- All default passwords for accounts must be constructed in accordance with the Password Policy.
- All accounts must have a password expiration that complies with the Password Policy.
- Accounts of individuals on extended leave (more than 30 days) will be disabled.
- All new user accounts that have not been accessed within 30 days of creation will be disabled.
- System Administrators or other designated staff:
    - are responsible for removing the accounts of individuals that change roles within or are separated from their relationship with
    - must have a documented process to modify a user account to accommodate situations such as name changes, accounting changes and permission changes
    - must have a documented process for periodically reviewing existing accounts for validity
    - are subject to independent audit review
    - must provide a list of accounts for the systems they administer when requested by authorized management or external auditors.