FETAKGOMO TUBATSE

LOCAL MUNICIPALITY

GROUP INFORMATION SECURITY POLICY

Council Resolution NR: OC148/2018

Version Control

Version	Date	Author(s)	Details
1.0			Group Information Security Policy

Approvals

DESIGNATION	NAME	SIGNATURE	DATE
Director :Cooperate Service			
Municipal Manager			
Mayor			

Contents

1. Introduction

Fetakgomo Tubatse Municipality's employees possess information that is sensitive and valuable, e.g., personally identifiable information, financial data, building plans, research, strategic planning and other information considered sensitive.

Some information is protected by South African laws or contractual obligations that prohibit its unauthorized use or disclosure.

The exposure of sensitive information to unauthorized individuals could cause irreparable harm to the Municipality or members of Fetakgomo Tubatse Municipality community, and could also subject the Municipality to fines or other government sanctions or even civil action.

Additionally, if FTLM's proprietary information were tampered with or made unavailable, it could impair Municipality's ability to do business, which will affect all employees and other key stakeholders.

The IT Unit is the guardian of the electronic and computer systems which all employees need to use, to do their work, and as such, the IT Unit requires all employees to diligently protect information as appropriate for its sensitivity level.

Failure by employees to comply with this policy may subject them to disciplinary measures and could ultimately result in termination of employment.

2. Terms and definitions

a. **IT** may refer to both Information Technology as well as the designated Unit

b. **Hardware** will refer to the CPU, printer, mouse, screen, consumer and third party technology (including, and without limitation: mobile devices like phones, i-Pads, Tablets and any like devices) and all related equipment or peripherals required or installed by the Greater Tubatse Municipality to operate IT systems.

c. **Software** will refer to in-house developed as well as registered and the Fetakgomo Tubatse Municipality approved software packages as authorized and installed by the IT Unit.

d. **Staff members** will refer to any permanent, temporary or contract workers who are performing specific duties for FTLM and are making use of computer equipment belonging to Fetakgomo Tubatse Municipality or themselves during the performance of those duties.

e. **Databases** will encompass any and all Third Party or Proprietary Database Platforms, and any reports, printouts, exports or screen captures obtained from said systems.

f. **Applications** refer to all front-end user interface systems, communicating with database management systems in the back-end.

3. Responsibilities

3.1 All Employees and Contractors

3.1.1 You may only access information needed to perform your legitimate duties as an employee and only when authorized by the appropriate manager.

3.1.2 You are expected to ascertain and understand the sensitivity of information to which you have access through training, other resources or by consultation with your manager or the IT Unit.

3.1.3 You may not in any way divulge, copy, release, sell, loan, alter or destroy any information except as authorized by the appropriate manager within the scope of your professional activities.

3.1.4 You must adhere to Fetakgomo - Greater Tubatse Municipality's requirements for any computers used to transact Fetakgomo - Greater Tubatse Municipality business - regardless of the sensitivity level of the information held on that system.

3.1.5 You must protect the confidentiality, integrity and availability of Fetakgomo Tubatse Municipality information as appropriate for the information's sensitivity levels, wherever the information is located, e.g. held on physical documents, stored on computer media, communicated over voice or data networks and exchanged in conversation, etc.

3.1.6 You must safeguard any physical key, ID card or computer/network account that allows you to access Fetakgomo Tubatse Municipality information. This includes creating difficult-to-guess computer passwords.

3.1.7 You must destroy or render unusable any confidential or highly confidential information contained in any physical document (e.g., memos, reports, microfilm) or any electronic, magnetic or optical storage medium (e.g., USB key, CD, hard disk, magnetic tape) before it is discarded.

3.1.8 You must report any activities that you suspect may compromise sensitive information to your supervisor.

3.1.9 Your obligation to protect sensitive information continues after you leave Fetakgomo Tubatse Municipality premises or employment.

3.1.10 While many South African laws create exceptions allowing for the disclosure of confidential information in order to comply with investigative subpoenas, court orders and other compulsory requests from law enforcement agencies, anyone who receives such compulsory requests should contact the Office of the Municipal Manager before taking any action.

3.1.11 If you are performing work in an office that handles information subject to specific security regulations, you will be required to acknowledge that you have read, understood and agreed to comply with the terms of this policy annually.

3.2 Managers and Supervisors

3.2.1 In addition to complying with the requirements listed above for all employees and contractors, managers and supervisors must:

3.2.1.1 Ensure that departmental procedures support the objectives of confidentiality, integrity and availability defined by the IT Unit and designees, and that those procedures are followed.

3.2.1.2 Ensure that restrictions are effectively communicated to those who use, administer, capture, store, process or transfer the information in any form, physical or electronic.

3.2.1.3 Ensure that each staff member understands his or her information security-related responsibilities.

3.3 Information Technology Unit

3.3.1 In addition to complying with the policy requirements defined for all employees, contractors, managers and supervisors, those who manage computing and network environments that are used to capture, store, process and/or transmit Fetakgomo Tubatse Municipality proprietary information, are responsible for ensuring that the requirements for confidentiality, integrity and availability are being satisfied within their environments.

This includes

3.3.1.1 Understanding the sensitivity level of the information that will be captured by, stored within, processed by, and/or transmitted through their technologies.

3.3.1.2 Developing, implementing, operating and maintaining a secure technology environment that includes:

3.3.1.3 A cohesive IT architectural policy.

3.3.1.4 Product implementation and configuration standards.

3.3.1.5 Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies Fetakgomo - Greater Tubatse Municipality security requirements.

3.3.1.6 An effective strategy for protecting information against generic threats posed by computer hackers that adhere to IT industry-accepted "best practices" for the technology.

3.3.1.7 Ensuring that staff members understand the sensitivity levels of the data being handled and the appropriate measures used to secure it.

4. Policy Framework

In the interests of simplicity, all the Information technology policies and procedures relevant and applicable to Fetakgomo Tubatse Municipality have been condensed into a smaller set of documents to be reviewed and understood by all employees.

4.1. IT Network End user IT Policies and Procedures

This document is applicable to all FTLM employees. It provides guidelines and procedures for completing any computer related tasks whilst in the employ of Fetakgomo Tubatse Local Municipality

The Document includes the following IT policies – applicable to all users on the IT systems

a. Hardware Allocation Policy
b. Hardware Usage Policy
c. Software Usage Policy
d. Internet and e-Mail Policy
e. IM and Social Media Policy
f. Confidentiality Policy
g. Personal Computer Equipment Policy
h. Telecommunications Policy
i. General Shared Drive Resources Policy
j. Backups Policy
k. Remote Access Policy
l. Loss/Theft and/or Damage Policy
m. Returning of Fetakgomo Tubatse Municipality Property Policy

4.2. PC and Electronic Device Acceptable Usage Policy

This policy governs the usage of any electronic device in use on any premises owned or rented by Fetakgomo Tubatse Municipality, whilst in the employment of Fetakgomo Tubatse Municipality

The policy provides summary guidelines regarding access to and disclosure of data on any of the Fetakgomo Tubatse Municipality electronic communication systems, and will help you to better determine how to use these systems in light of your own and the Municipality's privacy and security concerns.

The Policy Document is applicable to all users on the IT systems

4.3. Municipal and Contractor Policies and Procedures

This policy document describes the roles and responsibilities of any member of Fetakgomo Tubatse Municipality IT support team and any contractor they may be employed to assist with the efficient operation of the IT systems at Fetakgomo Tubatse Municipality

The document includes the following IT Policies:

a. Destruction of Hardware and Media Policy
b. Backups and Restoration Testing Policy
c. User Account Management Policy
d. Granting and Monitoring Administrative Rights Policy
e. User Account Review Policy
f. Network and Application Change Management Policy
g. Firewall Policy
h. Anti-Virus and Malware Policy
i. IT Ethics and Procurement Standards Policy
j. Network Vulnerability and Penetration Test Policy
k. IT Service Desk Policy

The Policy Document is applicable to all users on the IT systems

4.4. Contractor Confidentiality and non-Disclosure Agreement

A standard document specifying the responsibilities of any contractor providing outsourced IT services to Fetakgomo Tubatse Municipality

This Policy document is applicable to and must be completed by IT Contractors, temporary staff and visitors into the Server rooms at the various Fetakgomo Tubatse Municipality sites.

4.5. Policy Review

a. This policy shall be reviewed twenty four (24) months after the day of council approval.