

Blouberg Municipality



IT SECURITY POLICY

GLOSSARY

"**BLMITO**" Refers to Blouberg Local Municipality Information Technology Office staff members.

"**IT**" refers to Information Technology.

"**BLMITO- IT security Policy**" refers to Blouberg Local Municipality Information Technology Office Information Technology Security Policy.

"**BLM**" refers to Blouberg Local Municipality.

"**Network Devices**" refers to computers and devices interconnected by communications among users.

"**The municipality**" refers to Blouberg Local Municipality.

"**IR**" refers to Information Resources.

"**HR**" refers to Human Resource Management Division.

"**MFC**" refers to Multi-Function Copier

"**email**" refers to electronic mail

"**UPS**" refers to Uninterrupted Power Supply
"**BCP**" refers to Business Continuity Plan
"**DRP**" refers to Disaster Recovery Plan
"**MM**" refers to Municipal Manager

"**SLA**" refers to Service Level Agreement

"**Workstation**" refers to computers and laptops.

1. PREAMBLE

The Blouberg Information Technology Office (BLMITO) has developed the Information Technology Security Policy that shall apply to all Blouberg Municipality officials, its contractors, service providers, interns, students, councillors, and other authorized 3rd party entities that will need the municipality's IT network in order to perform respective duties on the network of BLMM. The purpose of this policy is to protect the municipality's Information Technology resources and to safeguard the confidentiality and integrity of Information, resources, data, ICT equipment and council documentations.

This BLMITO-IT security policy reflects the municipality's commitment to comply with the best practice to govern and protect the security of sensitive and confidential information. Wherever possible, this policy attempts to establish balance between the risks of loss of information resources. It includes provisions to reduce, as far as feasible, the risk of theft, fraud, destruction or other misuse of the municipality's information technology resources.

Administrative information processing, digital telecommunications and related technology are a critical business operation of the municipality. Inappropriate exposure of confidential and/or sensitive information, loss of data and inappropriate use of computer network systems can be minimized by complying with reasonable standard, attending to the proper design and control and control of information systems, and applying sanctions when violations of this IT security policy occur.

2. USER AWARENESS

- (1) IT Security is responsibility of everyone who uses the municipality's information technology resources.
- (2) In connection with the implementation of this policy, IT shall hold periodic training and awareness raising sessions throughout BLM in partnership with applicable stakeholders. Awareness shall be through workshops, desktop trainings or via email distribution to users.
- (3) It is the responsibility of key users to take privacy and security into consideration when evaluating the potential, the use of cloud-based IT solutions. In addition, staff that grant access to BLM IT systems need to ensure that authorized users are aware of this policy.
- (4) Every councillor, employee, contractor, and authorised 3rd party entity should become familiar with this policy's provisions and the importance of adhering to it when using the municipality's computers, networks, data, and other information resources.

- (5) Each user/holder is responsible for reporting any suspected breaches of security to the IT Manager.
- (6) Popularization of this policy will be conducted through presentation to all staff members.
- (7) All Municipality's computer, laptops, peripherals and computer workstations, terminals, telephones, facsimile machines, and other devices either owned by the municipality or authorised by municipality to connect to its networks are primarily for

Municipality business functions. As such, all information technology resource users within the municipality are expected to:

- (a) Respect the privacy of other users.
 - (b) Respect the rights of other users.
 - (c) Respect the intended use of resources and systems.
 - (d) Respect the integrity of the system or network.
 - (e) Adhere to all Municipality policies and procedures mandated by the BLMITO
- (8) All officials shall attend presentation of this policy and sign on the attendance register as acknowledgement of knowledge of the contents of this policy and repercussions of transgression

3. PURPOSE

- (a) The purpose of this policy is to safeguard the municipality's IT.
- (b) To put measures, control and processes that ensure adherence to this policy when carrying out municipal duties.
- (c) Users should be aware that they are discouraged to give access to other party's access to BLM systems, software, and applications; and
- (d) The risk of doing so lies with the users.

4. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY

- (a) Password policy.
- (b) Change management policy.
- (c) ICT Equipment policy
- (d) Network access policy
- (e) COBIT 5- Framework for the governance and Management of Enterprise IT 2012
- (D) ISO/IEC 20000
- (g) ISO/IEC 27000
- (h) KING IV — Corporate governance of Information and Communication Technology (ICT)
- (i) ITIL v3

5. SCOPE OF APPLICABILITY OF THE POLICY

- (a) This policy applies to every network user of BLM, systems, telephones, printers, peripherals, MFC's facsimile machines and other devices either owned by the municipality or authorised by the Municipality to connect to the networks.
- (b) It is also to every councillor, employee, contractor and authorised 3rd party entity accessing the municipality's networks and ICT resources.

6. ROLES AND RESPONSIBILITIES

- (a) BLMITO is responsible for ensuring that IR is maintained in compliance with the municipality's IT security policy and procedures.
- (b) Other service Providers whose systems are not managed by BLMITO are responsible for ensuring that their systems are maintained in compliance with the BLMITO IT security policy and procedures.
- (c) The IT Manager is responsible for monitoring compliance to the municipality's IT Security Policy.
- (d) All BLMITO team members are responsible to make sure that they are keeping systems in compliance with the municipality's IT security policy.
- (e) BLMITO budget will not be used to pay for ICT assets which have been lost due to negligence, carefree, misuse, misplaced, negligently broken and/or damaged.
- (D) ICT will provide minimum replacement of the equipment that has been lost, broken, damaged, misplaced, and misused: the bare minimum will be used desktop computer.
- (g) It is HRMs responsibility to inform BLMITO regarding staff terminations and all those officials and councillors that cease to serve in the municipality. This includes new appointments. This information is to be supplied to IT a month in advance where appropriate
- (h) Assets management will be the chief custodian of all ICT assets and should inform BLMITO of all the new ICT assets procured and barcoded.
- (i) BLMITO will inform assets management of the entire ICT asset movements' needs in writing and such interactions between assets management and IT must be in writing or email and asset section will record such movement in their assets register.
- (j) It is the sole responsibility of the ICT equipment and/or asset user to ensure that no ICT equipment and/or asset is removed by anyone including BLMITO team members without following proper procedures as contain in the IT Security Procedure Manual.
- (k) Revenue management will be the debt collector for any loss, negligent, damage, broken and misused ICT assets and equipment' s.
- (l) Revenue management to determine the depreciated value of the assets to be able to administer the repayment of the ICT asset and/or equipment after following all due processes.

- (m) Salary management will work in collaboration with revenue management to administer payment of the lost, damaged, broken, negligence and misuse of ICT asset and equipment
- (n) It is the responsibility of the Manager IT to ensure that there is continuity of services through the development of the development of backup systems, BCP and DRP, which will restore the critical services of BLM through SLA's.

7. ENFORCEMENT/LEGAL FRAMEWORK

- (a) Any employee found to have violated this policy may be subjected to disciplinary action, up to and including termination of employment.
- (b) Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations, and policy prescripts (this list is by no means exhaustive):
 - (i) The state Information Technology Act
 - (ii) SITA Amendment Act
 - (iii) Promotion of Access to information Act
 - (iv) Municipal Service Act
 - (v) Municipal Finance Management Act
 - (vi) National Archives Act
 - (vii) Protection of Government Information Act
 - (viii) Telecommunication Act.
 - (ix) Electronic Communication and Transaction Act
 - (x) Various other statutes
 - (xi) Any other application legislation, regulation, or policy

8. POLICY

(1) Data Backup

- (a) BLMITO will ensure a full backup is performed monthly.
- (b) BLMITO will perform daily incremental backups daily and stored away.
- (c) Backups will be scheduled to run automatically daily during off peak times.
- (d) Backup logs must be checked on a regularly to ensure successful completion of backups.
- (e) Cleaning of backup devices should be performed according to manufacturer's specification.
- (D) Complete backups must be stored off-site.
- (g) Backups must be validated and tested at least quarterly.
- (h) Only to work related information and official documents will be on BLM back up system
- (i) Under no circumstances will audio, video, and pictures be backed up unless written approval is obtained from the MM.

- (j) Under no circumstance will it be permitted that anyone be allowed to view, edit, modify, delete or temper with the information on the backup system unless written approval is obtained from the MM.
- (k) Under no circumstance shall anyone have access to other employee's information.
- (l) BLMITO will under no circumstance be required to perform or access any user's information without prior approval from the MM.

(2) Managing Passwords

Password leaks are dangerous since they can compromise the Municipality's entire infrastructure. Not only should passwords be secure so they will not be easily hacked, but they should also remain secret. For this reason, employees are to:

- (a) Choose passwords with at least eight characters (including capital and lower-case letters, numbers, and symbols) and avoid information that can easily guessed (e.g., birthdays).
- (b) Remember passwords instead of writing them down. If employees need to write their passwords, they are obliged to keep the paper or digital document confidential and destroy it when their work is done.
- (c) Exchange credentials only when necessary. When exchanging them in-person is not possible, employees should prefer the phone instead of email, and only if they personally recognize the person they are talking to.
- (d) Change their passwords every thirty (30) days.

(3) Data Transfers

Transferring data introduces security risks. Employees must:

- (a) Avoid transferring sensitive data (e.g., customer information, employee records) to other devices or accounts unless it is necessary. When mass transfer of such data is needed, we request employees to seek help from IT officials.
- (b) Share confidential data over the municipal network/system and not over public WI-FI or private network connections.
- (c) Ensure that the recipients of the data are properly authorized people or organizations and have adequate security policies.
- (d) Report scams, privacy breaches and hacking attempts.

(4) Use of cloud computing services

- (a) Notwithstanding the fact that a certain cloud service has been approved for use by IT, the fact that such a service requires proper encryption,

means that technical units must seek approval of the use of such service from IT Manager which will be responsible for ensuring that proper encryption is in place.

- (b) Use of cloud computing services involving Greater Giyani Municipality data must be formally authorized on a case-by-case basis by the IT Manager.
- (c) For confidential or internal data, cloud solutions are normally acceptable only if proper encryption (AES-256 or higher encryption standard) is implemented with encryption keys generated and stored at the approved service provider.
- (d) If proper encryption, pre-approved by IT, is not available, cloud services may not be used. Exception can be obtained with approval of the Council.
- (e) The use of cloud computing services must comply with all Greater Giyani Municipality Information Technology policies. (t) For public data, cloud solutions are acceptable.

(5) Risk assessment

The following non-exhaustive list of issues should be considered before considering any cloud computing solutions involving Greater Giyani Municipality data:

- (a) The IT priority needs of the municipality and the related business case, the type of information and data to be stored, their confidentiality and sensitivity (e.g., emails, old archival records, correspondence with third parties, HR or medical information, financial information, meeting records, etc.)
- (b) The region where the service provider or the cloud servers is located.
- (c) The type of cloud solutions and configurations available and their cost and efficiency
- (d) The available risk mitigation measures and mitigation costs for external, public and hybrid clouds, including through encryption of data, segregation of data, and appropriate contractual clauses.
- (e) Whether storage of the information and data in question requires the agreement of, or at least consultation with, staff and/or third parties.

(6) Risk Management

- (a) Encryption mechanisms
- (b) Physical segregation of BLM's records on dedicated servers at its request.
- (c) Development of special contractual terms and conditions to ensure the protection of BLM's privileges and immunities.

- (d) Appropriate Service Level Agreements with vendors.

(7) Physical Security

- (a) All servers must be constructed with concrete walls, raised floors and fire resistance doors.
- (b) All third-party vendor access to the server and switch room must be logged in a register in the format (Name, surname, company, purpose, Date and time) and must be accompanied by BLMITO official at all times
- (c) Where possible, server and switch room should be equipped with a temperature monitoring system which allows for alert to be sent by email or SMS when high temperature alarm is trigger
- (d) Log files must exist for equipment maintenance schedules according to manufacturer' s specification
- (e) All computer equipment's in the server and switches rooms must be connected to the UPS device
- (f) The UPS must be tested annually, and batteries checked for recommended use dates and physical defects
- (g) Where possible UPSs should be equipped with monitoring system which allows for alerts to be sent by email or SMS during power failure and low battery alarms
- (h) The backup generator should be checked on a weekly basis after every use
- (i) The backup generators should be tested on an annual basis
- (j) The backup generator should be services according to manufacturer's specification and a log should be kept
- (k) A fire detection system should be present in every server and switch room.
- (l) Where possible a fire preventions system (Halon or CO2) should be present in server and switch rooms
- (m) Before temporary off site removal of any computer equipment, a computer removal document must be filled in and approved.
- (n) Server rooms must be equipped with electronic access control devices and logs kept of all entries.
- (o) Switch rooms or cabinets must be locked at all times
- (p) No server rooms shall be used as offices, access to server rooms shall be controlled and be limited to session for which work is performed
- (q) No entry will be given to any official other than BLMITO official and/or in absence of BLMITO official
- (r) Access control register to the server room should be signed each time the is an entry into the server room.
- (s) All unused computer equipment must be stored in a secure location
- (t) Users are responsible for safe keeping of equipment assigned to them

- (u) Entry to server rooms shall be control by two entry methods i.e., lock and keypad and/or biometrics
- (v) Server rooms must be located in close proximity with BLMITO office or Offices
- (w) No user including 3rd party service provides will be given a local admin, network admin and/or domain admin security passwords
- (x) Access reports and information must be available and up to date at all times
- (y) All installation on workstations will be performed using local admins profile.

(8) User Account and Password Management

- (a) All accounts shall be reviewed at least quarterly to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status
- (b) The HRM will ensure that BLMITO be informed at least one month in advance of any new appointments. No user account will be created or modified without a signed New/Modified User Form
- (c) All user account will be deleted, and mailboxes deleted immediately by the BLMITO, upon an employee's departure from the municipality either by dismissal, transfer, resignation, retirement, death or any other form of departure as per HRM line Managers information. There shall be system to record terminations and new appointments and such information will form part of BLMITO monthly reports
- (d) An employee's access to a user account will be changed/modified by BLMITO, one the employee has transferred to a different division, in accordance with the employee's new job functions and requirements
- (e) All user accounts at the municipality are created as standard user accounts. This means that users have standard privileges to log onto the network, use network printers that have been assigned to them, access their email, and use the internet and any other privilege that is a core requirement of their job function.
- (f) Usernames are standardized and the employee's unique employee number is used to enable the user to log onto the network, and user's computer. Email addresses are also standardized with the employee's surname and initial, the user's full names may be used as an email address. The password that an employee uses to log onto the network will be applied to access the employees email account and internet applications.
- (g) The Mayor, The Speaker, The Chief Whip, full time councillors, interns and temporary appointed contractors will be issued with usernames and passwords, which will be operative until their service is terminated
- (h) Passwords must not contain the user's entire parts of the user Surname or employee number.

- (i) Passwords must contain characters from three of the following five categories:
 - (i) Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
 - (ii) Lowercase characters of European languages (a through sharps, with diacritic marks, Greek and Cyrillic characters)
 - (iii) Base 10 and (0 to 9)
 - (iv) Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asia languages.
 - (v) No alphanumeric characters: ~!@#\$%^&*~+\(){}[];:~""'<.>./
 - (vi) Passwords must never be written down on a piece of paper.
 - (vii) Never share passwords with anyone
 - (viii) Use different passwords for all user accounts.
 - (ix) Passwords should be changed every 30 days
 - (x) Officials shall not share their passwords with other officials
 - (xi) Keep your passwords safe and secret
 - (xii) No officials are allowed to show their passwords to BLMITO officials for any reason

(9) Virus Protection

- (a) Every system must be protected by anti-virus software and up to date
- (b) Configurations must allow for removable media to be scanned before allowing access on the municipality's network
- (c) A scheduled scan must be conducted on a monthly basis
- (d) Automatic updating must be configured to allow for the latest virus definitions in order to keep systems secure and protected against latest threats
- (e) Reporting must be enabled in order to monitor and managed threats
- (f) Anti-virus clients must be configured to prevent users from disabling antivirus protection
- (g) Anti-virus reports must be sent monthly with the monthly report.

(10) Firewall

- (a) All external connections must be protected by a firewall
- (b) Every firewall must be configured with deny-by-default policy
- (c) Internet access must be controlled by a proxy server.
- (d) Authentication to the firewall must be controlled by individual account access and the administrator username and password must be changed and renamed.
- (e) User account must be assigned with the lowest level of privileges required to perform duties.
- (f) Firewall software should be patched and updated on a regular basis.

(g) Logging of firewall data should be enabled

(h) Logs should be reviewed regularly

(i) Logs should be archived on a monthly basis

(j) Configuration logs should be backed up on a monthly basis and after every configuration change

(k) IT Manager should be alerted in the event of possible attacks and in the event of system failure.

(11) Patch Management

(a) Automated tools will scan for available patches and patches levels, which will be reviewed as specified in the patch management procedures document.

(b) Manual scans and reviews will be conducted on systems for which automated tools are not available

(c) Vendors supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied

(d) Where possible, patch will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems.

(e) Successful backups of mission critical systems will be verified prior to installation of patches and mechanism for reverting to the patch levels in effect prior to patching will be identified.

(f) Patches will be applied during an authorised maintenance windows in cases where the patch application will cause a service interruption for mission critical systems.

(g) Patches will be prioritized

(h) Logs will be maintained for all system categories (servers, secure desktops, ASCL, switches, etc.) indicating which devices have been patched. System logs help record the status of the systems and provide continuity among BLMITO officials. The log may be in paper or electronic form. Information to be recorded will include but is not limited to date of action, BLMITO official's name, and patches and patch numbers that were installed, problems encountered, and system administrator's remarks.

(i) In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels that were in effect before reloading started

(j) Authorised patches reports and statistics must be sent with monthly report on a monthly basis

(12) Remote Access Connections

- (a) A remote access connection is only allowed for server access

(13) Workstation Security

- (a) All workstations must be installed with Anti-virus software, and it must be updated before the workstation can be signed by the BLM officials

Users are not allowed to have administrative access on the workstations and laptops

- (b) Local administrator account must be removed
- (c) Use "my documents" folder must be redirected to a server share drive to enable backups to be performed.
- (d) Automatic updates must be configured to obtain the latest patched from the WSUS server
- (t) Security and event logs must be available for a minimum of 30 days
- (g) Any services that are not needed must be disabled
- (h) A screensaver password must be configured

(14) Server Security

- (a) All servers must have up to date antivirus, latest patches, drivers, and software
- (b) Physical access to servers must be limited to BLMITO officials and all changes to servers must be made in accordance with the change management policies and procedure manuals.
- (c) All users with administrative access must be documented
- (d) BLMITO officials will use their login credentials to log on to servers at all times
- (e) Automatic updates must be configured to obtain the latest patched from the applicable server
- (f) All volumes should be formatted with the NTFS file system
- (g) All events must be logged, and log files exported and archived
- (h) Log files should be reviewed regularly
- (i) All unneeded services must be disabled
- (j) All servers must be backup all times'
- (k) The server log on screen must have time out
- (l) No officials will use the server room as an office including BLMITO officials. It recommended that BLMITO offices be in close proximity to the server room.

(15) Client Data

- (a) User data folder must have permission enabled and only the owner of the folder and files and administrators should be allowed access to these folders

9. POLICY REVIEW


- (a) This policy shall be reviewed as when necessary.

10. POLICY APPROVAL

This policy was formulated by IT Division in consultation with the IT Steering Committee.

Authorised by Municipal Manager: Signature:  Date: 30/07/2024

Recommended by Portfolio Committee on Corporate Services

Signature:  Date: 30/07/2024

Approved by Municipal Council: Signature:  Date: 30/07/2024