



LOCAL GOVERNMENT SERVICE

INFORMATION TECHNOLOGY POLICIES

OFFICE OF THE HEAD OF LOCAL GOVERNMENT SERVICE
2017

CONTENTS

FOREWORD	2
1.0 INTRODUCTION	4
1.1 DEFINITIONS AND DISTINCTIONS:	4
1.2 OBJECTIVES	6
1.3 THE ICT MANAGEMENT DISCIPLINE	6
1.4 ICT RESOURCES CLASSIFICATION	8
2.0 ANTIVIRUS POLICY	9
3.0 APPLICATION IMPLEMENTATION POLICY	16
4.0 ASSET CONTROL POLICY.....	18
5.0 BACKUP POLICY.....	25
6.0 INCIDENT RESPONSE POLICY	29
7.0 INTERNET SECURITY POLICY.....	34
8.0 IT EQUIPMENT PURCHASE AND FAILURE PREVENTION POLICY	37
9.0 MOBILE COMPUTER POLICY	40
10.0 NETWORK DOCUMENTATION POLICY	46
11.0 PASSWORD POLICY	50
12.0 REMOTE ACCESS POLICY.....	54
13.0 SERVER DOCUMENTATION POLICY	57
14.0 SERVER MONITORING POLICY	61
15.0 SYSTEM LOCKDOWN POLICY.....	63
16.0 SYSTEM UPDATE POLICY.....	68
17.0 USER PRIVILEGE POLICY	72
18.0 WIRELESS USE POLICY	75
19.0 HUMAN RESOURCES MANAGEMENT INFORMATION SYSTEM POLICY	77
20.0 WEBSITE POLICY.....	83


FOREWORD

The information superhighway has now become an indispensable phenomenon in all facets of human endeavours in terms of communication and data management. The indispensability of the phenomenon could further be appreciated within the context of turning the entire world into a “Global Village” through the use of Internet and World Wide Web (WWW). The Internet and World Wide Web (WWW) phenomenon could be likened to a *Tsunami* which unceasingly sweeping across the entire world with high velocity creating both opportunities and threats in its wake. The opportunities are translated into the availability or accessibility of wide range of information/data with the click of a button. Such information/data facilitates the making of informed decisions by public actors and individuals for the good of society. Another added advantage is that it enhances easy communication in the form of social networking among others.

Notwithstanding the above, advantages there are equally inherent threats or risks, which individuals, organizations, and governments should take cognizance of. This brings to the fore the need for an Information Technology (IT) Policy in respect of computer use, network, software, IT security. Hence, this IT Policy sought to maximize the opportunities accruing from the use of IT within the Service on one hand and on the other attempt to reduce the inherent threats/risks to the barest minimum. This means users should adhere to the best practices as contained in this document to regulate and protect official information/data from abuse. To this end, the Local Government Service’s IT Policy is intended to provide the entire Service i.e. the Office of the Head of Local Government Service (OHLGS), Regional Co-ordinating Councils (RCCs), Metropolitan, Municipal and District Assemblies (MMDAs) with a *modus operandi* in information gathering, storage and use by staff in line with the best practice as previously noted.

Again, the Service is not unaware of the fluidity of information technology as a discipline. However, it is anticipated that the present policy could regulate the accessibility of information/data in accordance with the laid down rules and regulations, which the Service deems expedient in this slippery technological environment.

As the Head of Service, I kindly, implore all staff to acquaint themselves with the policy in its entirety for the enhancement of the security of our computers, data and other related electronic accessories.



Dr. CALLISTUS MAHAMA
HEAD OF LOCAL GOVERNMENT SERVICE

1.0 INTRODUCTION

This operational manual serves as a guideline for managing an integrated and structured approach to the deployment, exploitation, and management of ICT resources and services. Like other resources such as staff, capital and facilities, ICT services require planning, monitoring, controlling, and staffing that conform to international standards and best practices.

1.1 DEFINITIONS AND DISTINCTIONS:

- Information Technology (IT)
- Information and Communication Technology (ICT)
- Information Systems (IS)
- IT Management

a. Information Technology (IT)

- Describes the combination of computer technology (hardware and software) with telecommunication technology (data, image and voice networks).
- Information and Communication Technology (ICT) is the same as IT.

b. Information System (IS)

- Describes the processes, system, tools that work together to collect, process, store, retrieve, analyse and/ or distribute information.
- Note that IS may rely on information technology (IT) or not.
- IT improves IS

c. IT Management

- It encompasses the systems, people, processes and tools used to manage ICT resources for the good of the organization
- ICT management is a relatively new discipline.

- ICT is practised as a discipline like Accounting, Marketing and Human Resource (HR management)
- Like any other discipline, it has goals, policies and functions.
- ICT in organisation could be a core function, strategic or support function.

1.2 OBJECTIVES

The objectives of the Policies:

- To promote best practices to guide the deployment and exploitation of ICT within the LGS;
- To ensure data integrity for all users;
- To ensure the effective and efficient utilization of ICT facilities at LGS;
- To establish standard procedures for the purchase of compatible hardware and software appropriate to all users.
- To facilitate the enforcement of standards and best practices to guide the deployment and exploitation of ICTs within LGS.
- To monitor and evaluate the effective use of these procedures.

1.3 THE ICT MANAGEMENT DISCIPLINE

1.3.1 **DATA PROCESSING SYSTEM:** This is an information system that automates basic information processes – those that are well defined, structured and repetitive.

Example: Payroll, Maintaining Ledgers, Stock Control.

- It is normally used by clerical staff, data processing operators and line supervisors.
- Benefits: Cost savings through reduction of staff.

1.3.2 **MANAGEMENT INFORMATION SYSTEM (MIS):** This is a system that increases management effectiveness by satisfying information needs.

Example: Human Resource Data Analysis, Manpower Budgetary Control, Evidence based Decision making.

- It is normally used by managers and professionals.
- Benefits: Are difficult to quantify because they are mainly intangible – timeliness, accuracy to improve decision making and hence control.

1.3.3 **INFORMATION SYSTEM:** This is a system that improves competitiveness by changing the nature or conduct of business.

Example: Online access system for IPPD inputs forms.

- Benefits: Improves significantly the quality of the human resource database which in turn aids quick Human Resource management decision making

1.3.4 **BENEFITS OF ICT**

Generally, benefits of ICT could be any of the following:

(i) **Financial Benefits**

- Lower the cost of storing and retrieving data
- Reduce cost of operation.

(ii) **Organisational Benefits**

- Gain competitive advantage
- Fulfils regulatory or legal requirements
- Promote company/organisation values and strategic decisions.
- Improve customer service opportunities.
- Improved services delivery

(iii) **Operational Benefits**

- Increase productivity
- Improve work flow

- Save time
- Enhance information flow and access for coordination, planning research, and decision making and monitoring.

(iv) **Technological Benefits**

- Maintain or improve system reliability, system security, system performance.
- Keep systems current in terms of configuration or version.
- Protect current investment in technology.
- Lower technical support costs.
- Facilitate technical support activities
- Meet service level obligations
- Facilitate system utilization – improving ease of use

The Benefits depend on the type of IT system.

1.4 ICT RESOURCES CLASSIFICATION

ICT Resources may be classified as follows:

- Hardware Systems;
- Networks and Telecoms;
- Software;
- Data and
- People ware

2.0 ANTIVIRUS POLICY

2.1 Overview

This policy is an internal IT policy which defines anti-virus policy on every computer including how often a virus scan is done, how often updates are done, what programs will be used to detect, prevent, and remove malware programs. It defines what types of files attachments are blocked at the mail server and what anti-virus program will be run on the mail server. It may specify whether an anti-spam firewall will be used to provide additional protection to the mail server. It may also specify how files can enter the trusted network and how these files will be checked for hostile or unwanted content. For example it may specify that files sent to the enterprise from outside the trusted network be scanned for viruses by a specific program.

2.2 Purpose

This policy is designed to protect the organizational resources against intrusion by viruses and other malware.

2.3 Anti-Virus Policy

The MMDA or RCC will use a single anti-virus product for anti-virus protection. The following minimum requirements shall remain in force.

1. The anti-virus product shall be operated in real time on all servers and client computers. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per day on all user controlled workstations and servers.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

2.4 Email Server Policy

The email server will have additional protection against malware since email with malware must be prevented from entering the network.

2.5 Email Malware Scanning

In addition to having the standard anti-virus program, the email server or proxy server will additionally include anti – malware which will be used to scan all email for viruses and/or malware. This scanner will scan all email as it enters the server and scan all email before it leaves the server. In addition, the scanner may scan all stored email once per week for viruses or malware.

When a virus is found or malware is found, the policy shall be to delete the email and not to notify either the sender or recipient. The reason for this is that most viruses fake the sender of the email and sending them a notice that they sent a message with a virus may alarm them unnecessarily since it would not likely be true. It would simply cause an additional help desk call by the notified person and most likely waste system administrator's time needlessly. Notifying the recipient that someone tried to send them a virus would only alarm them needlessly and result in an increased number of help desk calls.

2.6 Blocked Attachment Types

The e-mail server or proxy server will block all emails with attachment types listed below. This is because these attachment types are dangerous containing active content which may be used to infect a computer with hostile software or because these attachment types are commonly successfully used by virus programs or malware to spread.

1. ade - Microsoft Access project extension can contain executable code.
2. adp - Microsoft Access project can contain executable code.
3. app - Microsoft FoxPro application is executable code.
4. asp - Active server pages
5. bas - Basic program source code is executable code.
6. bat - Batch file which can call executable code.
7. chm - Compiled HTML help file can contain executable code.
8. cmd - Windows NT command script file is executable code.
9. com - Command file program is executable code.
10. cpl - Control panel extension
11. dll - Dynamic link library is executable code. Could be placed on your system then run by the system later.
12. exe - Binary executable program is executable code.
13. fpx - Microsoft FoxPro is executable code.

14. hlp - Help file
15. hta - HTML program
16. inf - Setup information
17. ins - Internet naming service
18. isp - Internet communication settings
19. js - JavaScript file
20. jse - JavaScript encoded file
21. ksh - Unix shell file
22. lnk - Link file
23. mda - Microsoft Access add-in program
24. mdb - Microsoft Access program
25. mde - Microsoft Access MDE database
26. mdt - Microsoft Access file
27. mdw - Microsoft Access file
28. mdz - Microsoft Access wizard program
29. msc - Microsoft Common Console document
30. msi - Microsoft windows installer package
31. msp - Windows Installer patch
32. mst - Visual Test source files
33. ops - FoxPro file
34. pcd - "Photo CD image or Microsoft Visual Test compiled script"
35. pif - "Shortcut to MS-DOS program"
36. prf - "Microsoft Outlook Profile Settings"
37. prg - "FoxPro program source file"
38. reg - Registry files
39. scf - "Windows Explorer Command file"
40. scr - Screen saver
41. sct - Windows® script component
42. shb - Document shortcut
43. shs - Shell scrap object
44. url - Internet address
45. vb - Visual Basic file
46. vbe - Visual Basic encoded script file
47. vbs - Visual Basic file
48. wsc - Windows script component
49. wsf - Windows script file
50. wsh - Windows script host settings file

51. xsl - XML file may contain executable code
52. zip - Many viruses are commonly zipping files to keep them from being scanned and providing instructions to users about how to run the attachment. Many users still do this so to secure the network; it has become necessary to block this attachment type.

Do not depend on your anti-virus software on each computer to prevent these viruses. Viruses have a period of time when they spread unrecognized by anti-virus software. Blocking these file attachments will prevent many trouble calls. Give the users a work around for your network to get some of their files sent to other organizations. Your solution will depend on your network and the software that is being used to block the file attachments. In one case we renamed the file to another type and instructed the recipient to rename it back to the original name before using it. This will not work in all cases since some file blocking software senses the actual file type regardless of its named file extension.

When an email breaks the rules and contains an illegal file attachment your policy should define one of the following to be done:

1. Delete the email and notify neither the sender nor the recipient. The problem with doing this is in the fact that people may be trying to send legitimate files to each other and have no way of knowing their communication attempts are failing. Training by letting users know what files are blocked can help remedy this problem
2. Delete the email and notify the sender - This will notify senders when their emails do not go through, but it will also notify senders who really did not send an email (when a virus spoofed them as the sender) that they sent an email with an illegal attachment. This can cause more additional help desk requests and questions for the administrator on the spoofed sender's side.
3. Delete the email and notify the sender and recipient. - This would have all the drawbacks of the above policy but would also increase help desk calls in your organization.
4. Remove the attachment and let the email go through. - This would let the receiver know that someone tried to send them an illegal attachment. If the attempt was a legitimate one, they could contact the sender and tell them what to do to get the attachment sent. This policy would very likely cause your organization's help desk calls to increase with users calling to ask questions about why someone is trying to send them these files.

There is no ideal policy here and your system administrators must choose the best method depending on the situation being experienced by your assembly. It is advisable to use the first option and provide training to users so they know which files are blocked and what the work around is for this situation.

2.7 Proxy or Anti-Spam Server

To increase mail security, many organizations are adding an anti-spam server or proxy mail server to their network. This reduces their mail server to the threat of being intruded upon and an anti-spam server can significantly reduce the load on the mail server, not to mention the reduction of spam. Your organization should decide whether to use one of these types of servers or whether to use a service to prevent spam. The service or devices used for this purpose should be defined in this policy. Periodic updates should also be defined and the person who manages the additional servers or is the point of contact for the services should be defined.

2.8 File Exchange Policy

This part of the policy specifies methods that are allowed to be used when files are sent into the network by members of the public or employees of the organization. It specifies:

1. All legitimate methods used including:
 1. FTP transfer to a FTP server.
 2. File transfer to a Web server with a legitimate file upload program.
 3. Any other method.
2. The method and type of software to be used to scan the files for hostile content before they are completely transferred into the network. It will also specify the update frequency for the scanning software.
3. The point in time when the files will be scanned.

2.9 Network Exploit Protection

This policy should specify how hostile software that uses network exploits should be prevented. This policy will not cover system updates but may refer to the system update policy. This policy combined with other quoted policies should prevent worms from entering the network. This policy may also refer to the remote user policy and mobile computer policy.

This policy will specify that all systems be protected by a firewall any time they are connected to the internet. It would specify that systems on the organizational network be connected to a part of the network that is protected from the internet or untrusted network by an approved firewall system. It will also specify or refer to policy that requires computers operating outside the organizational network to have a local firewall software program operational at all times when these computers are connected to the internet. It should specify one or more acceptable software firewall products. This policy may refer to the mobile computer policy which may require users of mobile computers to have their computers checked for malware before connecting to the main network.

2.10. Other Malware Policy

This policy should cover any other possible malware including adware and spyware. It may specify methods to prevent and remove this type of malware. It may specify acceptable prevention and removal software. If the anti-virus product is a product that also handles other types of malware such as adware or spyware, it should be stated here.

Applicable Training

1. Blocked email attachments
2. How viruses work and avoidance
3. Adware and spyware avoidance

2.11. Use of Removable Storage Devices

All removable storage drives should be scanned by the user before usage.

2.12. Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

In the case that this policy is not being adhered to, the incident must be reported to the Head of Service or the Director RSIM or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

3.0 APPLICATION IMPLEMENTATION POLICY

3.1 Overview

This policy is to be used to assess the security impact of new applications. When new applications are developed to provide new functionality to customers or internal groups, the impact of the new functionality must be assessed in order to keep the network stable. Starting with a data assessment process will help this process flow smoothly.

3.2 Purpose

This policy is designed to protect the organizational resources on the network by defining requirements for new applications in the organization. This policy requires a security assessment including an assessment of data security levels, media the data will travel over, a risk evaluation, and determination of system requirements which will mitigate the most serious part of additional security risks.

3.3 Process

Customers shall work together with application developers and computer security experts to assess data requirements for any new applications. Customers shall specify their requirements for the applications and application developers will work with the customer to identify and categorize data according to the Application Development Security Assessment Process.

Once the data and application requirements are established, computer security personnel can then evaluate risk and determine methods, processes, equipment, and procedures to mitigate known risks. The computer security personnel, customers, and application developers will work together to provide required and reasonable access capability to systems and data both during development and final project implementation while providing the best computer security possible for a reasonable cost. Under no circumstances should the overall security of the network be seriously compromised for the benefit of any project.

The data assessment, risk evaluation, and system requirements should be done early in the project life cycle since without this information, the overall cost of the project cannot be accurately assessed.

The security assessment shall be conducted according to the Security Assessment Questionnaire and data shall be evaluated according to the Data Assessment Process document.

3.4 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

4.0 ASSET CONTROL POLICY

4.1 Overview

All employees and personnel that have access to organizational computer systems must adhere to the IT asset control policy defined below in order to protect the security of the network, protect data integrity, and protect and control computer systems and organizational assets. The asset control policy will not only enable Local Government Service assets to be tracked concerning their location and who is using them but it will also protect any data being stored on those assets. This asset policy also covers disposal of assets.

IT assets should not be confused with nor tracked with other organizational assets such as furniture. One of the main reasons to track IT assets other than for property control and tracking is for computer security reasons. A special IT asset tracking policy will enable the organization to take measures to protect data and networking resources.

This policy will define what must be done when a piece of property is moved from one building to another or one location to another. This policy will provide for an asset tracking database to be updated so the location of all computer equipment is known. This policy will help network administrators protect the network since they will know what user and computer is at what station in the case of a worm infecting the network. This policy also covers the possibility that data on a computer being moved between secure facilities may be sensitive and must be encrypted during the move.

4.2 Purpose

This policy is designed to protect the Assemblies resources on the network by establishing a policy and procedure for asset control. These policies will help prevent the loss of data or organizational assets and will reduce risk of losing data due to poor planning.

4.3 Assets Tracked

This section defines what IT assets should be tracked and to what extent they should be tracked.

4.3.1 IT Asset Types

This section categorized the types of assets subject to tracking.

1. Desktop workstations
2. Laptop mobile computers
3. Printers, Copiers, FAX machines, multifunction machines
4. Handheld devices
5. Scanners
6. Servers
7. Firewalls
8. Routers
9. Switches
10. Memory devices
11. External hard drives

4.3.2 Tracking Assets

Assets which cost less than one hundred (100) Ghana Cedis shall not be tracked specifically including computer components such as video cards or sound cards. However, assets which store data regardless of cost shall be tracked. These assets include:

1. Hard Drives
2. Temporary storage drives
3. Tapes with data stored on them including system backup data.
4. Although not specifically tracked, other storage devices including CD ROM disks and floppy disks are covered by this policy for disposal and secure storage purposes.

4.3.3 Small Memory Devices

Small memory storage assets will not be tracked by location but by trustee. These assets include:

1. Floppy disks
2. CD ROM disks
3. Memory sticks

If these types of devices are permitted for some employees, the trustee of the device must sign for receipt of these devices in their possession. All employees must also

agree to handle memory sticks, floppy disks, and CD ROM disks in a responsible manner and follow these guidelines:

1. Never place sensitive data on them without authorization. If sensitive data is placed on them, special permission must be obtained and the memory device must be kept in a secure area.
2. Never use these devices to bring executable programs from outside the network without authorization and without first scanning the program with an approved and updated anti-virus and malware scanner. Any program brought into the network should be on the IT department list of approved programs.

The Memory Device Trustee agreement allows employees to sign for receipt of these devices and agree to handle these devices in accordance with the terms of this policy. This form must be submitted by all employees that will work with any organizational data when the employee begins working for the organization. It will also be submitted when an employee receives one or more memory sticks, temporary storage drives, or data backup drives.

4.3.4 Asset Tracking Requirements

1. All assets must have an ID number. Either an internal tracking number will be assigned when the asset is acquired or the use of Manufacturer ID numbers must be specified in this policy.
2. An asset tracking database shall be created to track assets. It will include all information on the Asset Transfer Checklist table and the date of the asset change.
3. When an asset is acquired, an ID will be assigned for the asset and its information shall be entered in the asset tracking database.

4.4 Transfer Procedure:

1. **Asset Transfer Checklist** - When an asset type listed on the Asset Types list is transferred to a new location or trustee, the IT Asset Transfer Checklist must be filled out by the trustee of the item and approved by an authorized representative of the organization. The trustee is the person whose care the item is in. If the item is a workstation, then the trustee is the most common user of

the workstation. For other equipment, the trustee is the primary person responsible for maintenance or supervision of the equipment.

The trustee must fill out the Asset Transfer Checklist form and indicate whether the asset is a new asset, moving to a new location, being transferred to a new trustee, or being disposed of. The following information must be filled in:

1. Asset Type
2. ID number
3. Asset Name
4. Current Location
5. Designated Trustee
6. New Location
7. New Trustee
8. Locations of Sensitive Data

Once the trustee fills out and signs the Asset Transfer Checklist form an authorized representative must sign it.

2. **Data entry** - After the Asset Transfer Checklist is completed, it will be given to the asset tracking database manager. The asset tracking database manager will ensure that the information from the forms are entered into the asset tracking database within one week.
3. **Checking the database** - Managers who manage projects that affected equipment location should check periodically to see if the assets that recently were moved were added to the database. The database should provide a recent move list which can be easily checked. Managers should check the database weekly to be sure assets moved within the last 2 or 3 weeks are included in the database.

4.5 Asset Transfers

This policy applies to any asset transfers including the following:

1. Asset purchase
2. Asset relocation
3. Change of asset trustee including when an employee leaves or is replaced.

4. Asset disposal

In all these cases the asset transfer checklist must be completed.

4.6 Asset Disposal

Asset disposal is a special case since the asset must have any sensitive data removed prior to disposal. Any data storage devices. The manager of the user of the asset must determine what the level of maximum sensitivity of data stored on the device is. Below is listed the action for the device based on data sensitivity according to the data assessment process.

1. **None (Unclassified)** - No requirement to erase data but in the interest of prudence normally erase the data using any means such as reformatting or degaussing.
2. **Low (Sensitive)** - Erase the data using any means such as reformatting or degaussing.
3. **Medium (Confidential)** - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques.
4. **High (Secret)** - The data must be erased using an approved technology to make sure it is not readable using special hi technology techniques. Approved technologies are to be specified in a Media Data Removal Procedure document by asset type including:
 1. Floppy disk
 2. Memory stick
 3. CD ROM disk
 4. Storage tape
 5. Hard drive.
 6. RAM memory
 7. ROM memory or ROM memory devices.

4.8. Media Use

This policy defines the types of data that may be stored on removable media and whether that media may be removed from a physically secure facility and under what conditions it would be permitted. Removable media includes:

1. Floppy disk
2. Memory stick
3. CD ROM disk
4. Storage tape

Below is listed the policy for the device based on the rated data sensitivity of data stored on the device according to the data assessment process.

1. Unclassified - Data may be removed with approval of the first level manager and the permission is perpetual for the employee duration of employment unless revoked. The device may be sent to other offices using any public or private mail carrier.
2. Sensitive - Data may only be removed from secure areas with the permission of a director level or higher level of management and approvals are good for one time only.
3. Confidential - The data may only be removed from secure areas with permission of a Director or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
4. Secret - The data may only be removed from secure areas with the permission from the Office of the Head of Local Government Service or higher level of management. There must be some security precautions documented for both the transport method and at the destination.
5. Top secret - The data may never be removed from secure areas.

4.9. Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

5.0 BACKUP POLICY

5.1 Overview

This policy defines the backup policy for computers within the Local Government Service which are expected to have their data backed up. These systems are typically servers but are not necessarily limited to servers. Servers expected to be backed up include the file server, the mail server, and the web server.

5.1 Purpose

This policy is designed to protect data in the organization to be sure it is not lost and can be recovered in the event of an equipment failure, intentional destruction of data, or disaster.

5.2 Scope

This policy applies to all equipment and data owned and operated by the organization.

5.3 Definitions

1. **Backup** - The saving of files onto magnetic tape or other offline mass storage media for the purpose of preventing loss of data in the event of equipment failure or destruction.
2. **Archive** - The saving of old or unused files onto magnetic tape or other offline mass storage media for the purpose of releasing on-line storage room.
3. **Restore** - The process of bringing off line storage data back from the offline media and putting it on an online storage system such as a file server.

5.4 Timing

Full backups are performed nightly on Monday, Tuesday, Wednesday, Thursday, and Friday. If for maintenance reasons, backups are not performed on Friday, they shall be done on Saturday or Sunday.

5.5 Tape Storage

There shall be a separate or set of tapes for each backup day including Monday, Tuesday, Wednesday, and Thursday. There shall be a separate or set of tapes for each Friday of the month such as Friday1, Friday2, etc. Backups performed on Friday or weekends shall be kept for one month and used again the next month on the applicable Friday. Backups performed Monday through Thursday shall be kept for one week and used again the following appropriate day of the week.

5.6 Tape Drive Cleaning

Tape drives shall be cleaned weekly and the cleaning tape shall be changed monthly.

5.7 Monthly Backups

A monthly backup tape shall be made using the oldest backup tape or tape set from the tape sets.

5.8 Age of tapes

The date each tape was put into service shall be recorded on the tape. Tapes that have been used longer than 9 months shall be discarded and replaced with new tapes.

5.9 Responsibility

The IT department manager shall delegate a member of the IT department to perform regular backups. The delegated person shall develop a procedure for testing backups and test the ability to restore data from backups on a monthly basis.

5.10. Testing

The ability to restore data from backups shall be tested at least once per month.

5.11. Data Backed Up

Data to be backed up include the following information:

1. User data stored on the hard drive.
2. System state data
3. The registry

Systems to be backed up include but are not limited to:

1. File server
2. Mail server
3. Production web server
4. Production database server
5. Domain controllers
6. Test database server
7. Test web server

5.12. Archives

Archives are made at the end of every year in December. User account data associated with the file and mail servers are archived one month after they have left the organization.

5.13. Restoration

Users that need files restored must submit a request to the help desk. Include information about the file creation date, the name of the file, the last time it was changed, and the date and time it was deleted or destroyed.

5.14. Tape Storage Locations

This policy may contain descriptions about how various systems and types of systems are backed up such as Windows or UNIX systems. Offline tapes used for nightly backup shall be stored in an adjacent building in a fireproof safe. Monthly tapes shall be stored across town in our other facility in a fireproof safe.

5.15. Storage Device for ICT Staff

External hard drives should be provided for each IT personnel in the IT department.

5.16. Network Storage Device A network storage device may be procured for auto update of files if required.

5.17. Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

6.0 INCIDENT RESPONSE POLICY

6.1 Overview

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan document discusses how information is passed to the appropriate personnel, assessment of the incident, minimizing damage and response strategy, documentation, and preservation of evidence. The incident response plan will define areas of responsibility and establish procedures for handling various security incidents. This document discusses the considerations required to build an incident response plan.

6.2 Purpose

This policy is designed to protect the Local Government Service resources against intrusion.

6.3 Incident Response Goals

1. Verify that an incident occurred.
2. Maintain or Restore Business Continuity.
3. Reduce the incident impact.
4. Determine how the attack was done or the incident happened.
5. Prevent future attacks or incidents.
6. Improve security and incident response.
7. Prosecute illegal activity.
8. Keep management informed of the situation and response.

6.4.1 Incident Definition

An incident is any one or more of the following:

1. Loss of information confidentiality (data theft)
2. Compromise of information integrity (damage to data or unauthorized modification).
3. Theft of physical IT asset including computers, storage devices, printers, etc.
4. Damage to physical IT assets including computers, storage devices, printers, etc.
5. Denial of service.
6. Misuse of services, information, or assets.

7. Infection of systems by unauthorized or hostile software.
8. An attempt at unauthorized access.
9. Unauthorized changes to organizational hardware, software, or configuration.
10. Reports of unusual system behavior.
11. Responses to intrusion detection alarms.

6.5 Incident Planning

In the incident response plan, do the following:

1. Define roles and responsibilities
2. Establish procedures detailing actions taken during the incident.
 - Detail actions based on type of incident such as a virus, hacker intrusion, data theft, system destruction.
 - Procedures should consider how critical the threatened system or data is.
 - Consider whether the incident is ongoing or done.

6.6 Incident Response Life cycle

1. Incident Preparation

1. Policies and Procedures
 - Computer Security Policies - These involve many policies including password policies, intrusion detection, computer property control, data assessment, and others.
 - Incident Response Procedures
 - Backup and Recovery Procedures
2. Implement policies with security tools including firewalls, intrusion detection systems, and other required items.
3. Post warning banners against unauthorized use at system points of access.
4. Establish Response Guidelines by considering and discussing possible scenarios.
5. Train users about computer security and train IT staff in handling security situations and recognizing intrusions.
6. Establish Contacts - Incident response team member contact information should be readily available. An emergency contact procedure should be

established. There should be one contact list with names listed by contact priority.

7. Test the process.
2. **Discovery** - Someone discovers something not right or suspicious. This may be from any of several sources:
 1. Helpdesk
 2. Intrusion detection system
 3. A system administrator
 4. A firewall administrator
 5. A business partner
 6. A monitoring team
 7. A manager
 8. The security department or a security person.
 9. An outside source.
 10. The IT department
3. **Notification** - The emergency contact procedure is used to contact the incident response team.
4. **Analysis and Assessment** - Many factors will determine the proper response including:
 1. Is the incident real or perceived?
 2. Is the incident still in progress?
 3. What data or property is threatened and how critical is it?
 4. What is the impact on the business should the attack succeed? Minimal, serious, or critical?
 5. What system or systems are targeted, where are they located physically and on the network?
 6. Is the incident inside the trusted network?
5. **Response Strategy - Determine a response strategy.**
 1. Is the response urgent?
 2. Can the incident be quickly contained?
 3. Will the response alert the attacker and do we care?
6. **Containment** - Take action to prevent further intrusion or damage and remove the cause of the problem. May need to:
 1. Disconnect the affected system(s)

2. Change passwords.
3. Block some ports or connections from some IP addresses.
7. **Prevention of re-infection**
 1. Determine how the intrusion happened - Determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.
 2. Take steps to prevent an immediate re-infection which may include one or more of:
 1. Close a port on a firewall
 2. Patch the affected system
 3. Shut down the infected system until it can be re-installed
 4. Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
 5. Change email settings to prevent a file attachment type from being allowed through the email system.
 6. Plan for some user training.
 7. Disable unused services on the affected system.
8. **Restore Affected Systems** - Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following
 1. Re-install the affected system(s) from scratch and restore data from backups if necessary. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system.
 2. Make sure users change passwords if passwords may have been sniffed.
 3. Be sure the system has been hardened by turning off or uninstalling unused services.
 4. Be sure the system is fully patched.
 5. Be sure real time virus protection and intrusion detection is running.
 6. Be sure the system is logging the correct items
9. **Documentation** - Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.
10. **Evidence Preservation** - Make copies of logs, email, and other documentable communication. Keep lists of witnesses.

11. **Notifying proper external agencies** - Notify the police if prosecution of the intruder is possible.
12. **Assess damage and cost** - Assess the damage to the organization and estimate both the damage cost and the cost of the containment efforts.
13. **Review response and update policies** - Plan and take preventative steps so the intrusion cannot happen again.
 1. Consider whether an additional policy could have prevented the intrusion.
 2. Consider whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
 3. Was the incident response appropriate? How could it be improved?
 4. Was every appropriate party informed in a timely manner?
 5. Were the incident response procedures detailed and cover the entire situation? How can they be improved?
 6. Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
 7. Have changes been made to prevent a new and similar infection?
 8. Should any security policies be updated?
 9. What lessons have been learned from this experience?

6.7 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Directors of the Metropolitan, Municipal or District Assemblies.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

7.0 INTERNET SECURITY POLICY

7.1 Overview

This internet connection policy has components of a user compliance policy and an internal IT policy. The user compliance section specifies how users are allowed to connect to the internet and provides for IT department approval of all connections to the internet or other private network. It requires all connections such as connections by modems or wireless media to a private network or the internet be approved by the IT department and what is typically required for approval such as the operation of a firewall to protect the connection.

This internet connection policy requires users to use the internet for business only and requires users to avoid going to malicious web sites which could compromise security. It informs the users that their internet activity may be logged and monitored and defines whether user activity on the network will be logged and to what extent. It specifies what system will be used to prevent unauthorized viewing of sites and what system will log internet usage activity. Defines whether a proxy server will be used for user internet access. It defines how the network will be protected to prevent users from going to malicious web sites.

7.2 Purpose

This policy is designed to protect the organizational resources against intrusion by malware that may be brought into the network by users as they use the internet. It is also designed to prevent unauthorized and unprotected connections to the internet which may allow a host of unsafe content to enter the organizational network and compromise data integrity and system security across the entire network.

7.3 Physical Internet Connection

All physical internet connections or connections to other private networks shall be authorized and approved by the IT department. Most users will access the internet through the connection provided for their office by the IT department. Any additional connections must be approved by the IT department. These additional connections include but are not limited to:

1. Modem connection from a computer or communication device which may allow a connection to the network.
2. Any multipurpose printing and FAX machines which have both a phone and network connection must be examined and approved for use by the IT department.
3. Wireless access points or devices with wireless capability are not allowed unless approved by the IT department. If any computers or other devices have wireless capability, the wireless capability must be turned off before connecting to the network unless it is approved for wireless operation by the IT department when connected to the network.

Any additional internet connections not provided by the IT department must be reviewed and approved by the IT department. Typically any additional connections from the organizational network to the internet or other private network will require.

1. An IT department approved firewall operating at all times and properly configured.
2. Some communications through the connection may require encryption subject to a review of data to be transmitted by the IT department.

7.4 Use of the Internet

1. All employee use of the internet shall be for business purposes only.
2. Employee use of the internet may be monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.
3. Employees are urged to use caution when visiting unknown internet sites and through user training set and keep their browser configured to IT approved standards in order to protect against infections of malware. Employees will be trained in the latest IT approved standards to protect against malware when appropriate.

7.4 Internet Control and Logging System

A system will be required to operate on the network with the following capabilities:

1. The ability to prevent users from visiting inappropriate, pornographic, or dangerous web sites. It will have its database of categorized websites updated regularly.
2. The ability to log user internet activity including:
 1. Time of the internet activity.
 2. Duration of the activity.
 3. The website visited.
 4. Data and type of data downloaded
 5. Whether the system will cache web pages to increase the internet connection speed. This requires a proxy server.
3. The system (will | will not) require a login ID or it will use the current network login to identify users.

This same system will not require an additional login ID and will use Active Directory to identify internet users. The system shall be able to log the time of internet activity, duration of the activity, the website visited, any data downloaded and the type of data downloaded. The system will cache web pages.

7.5 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

8.0 IT EQUIPMENT PURCHASE AND FAILURE PREVENTION POLICY

8.1 Overview

This IT Equipment Purchase and Failure Prevention policy provides a guideline for the purchase of IT equipment when the equipment supports organizational identified critical services. This policy will name critical services and provide a guideline for purchasing technologies that are failure tolerant.

8.2 Purpose

The purpose of this policy is to ensure that critical services are not interrupted by a single common failure. It provides standard guidelines to allow IT equipment purchased for essential services to have reliability built into the equipment. This is to prevent service outage for critical services.

8.3 Scope

This policy covers any computers providing critical services to the organization.

8.4 Critical Services

Critical services which are required for normal operation of the organization include:

1. File sharing service on a file sharing server.
2. Web services to the internet
3. Email services
4. Database services for internal users and critical external applications.
5. Critical external application servers.
6. Domain controller servers
7. Firewall to connect these services to the internet.
8. Intranet Servers.

Any server or equipment that supports these services should adhere to this policy including connection equipment from the internet to these services.

8.5 Equipment Requirements

All critical services are required to utilize redundant technologies including:

1. Dual power supplies on all servers providing critical services.
2. RAID disk arrays to prevent one disk failure from interrupting services
3. Uninterruptable power supplies that can provide power for a minimum of 1 hour to servers operating critical services in the event of a power outage.

8.6 Additional Requirements

For services that are critical for income or operations that cannot be interrupted the following technologies are also recommended:

1. A backup generator to ensure that long term power outages cannot interrupt service.
2. More than one server for the same service where the servers use clustering or load balancing technology.

8.7 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

9.0 MOBILE COMPUTER POLICY

9.1 Overview

This policy defines the use of mobile computers in the Local Government Service. It defines:

1. The process that mobile computers must meet to enter the corporate network when being brought into a building owned by the organization
2. How mobile computers and devices will be protected while outside the organizational network.
3. The process that mobile computers must meet to leave the corporate network. Both the device and any sensitive data should be password protected.

9.2 Purpose

This policy is designed both to protect the confidentiality of any data that may be stored on the mobile computer and to protect the organizational network from being infected by any hostile software when the mobile computer returns. This policy also considers wireless access.

9.3 Scope

This policy covers any computing devices brought into the organization or connected to the organizational network using any connection method. This includes but is not limited to desktop computers, laptops, and palm pilots.

9.4 Responsibility

The user of the mobile computer will accept responsibility for taking reasonable safety precautions with the mobile computer and agrees to adhere to this policy. The computer user will not be allowed to have administrative rights unless granted special exception by the network administrator. The user of the computer agrees not to use the mobile computer for personal business and agrees to abide by the organizational computer usage policy.

9.5 Connection Terms

1. Devices connected to the organizational network must be determined to be a benefit to the organization rather than convenience by the designated IT manager.
2. All mobile devices owned by the organization or allowed on the organization network must be identified by their MAC address to the IT department before being connected. (Possibly require static IP address)
3. The device must meet the computer connection standards described in the following section.
4. The device operator must be identified by name and contact information to the IT department.
5. The computer device operator must be familiar with the organization's acceptable use policy.
6. Devices not owned by the organization are subject to a software audit to be sure no software that could threaten the network security is in operation. All computing devices are subject to a software audit at any time.
7. Access rights to the organizational network cannot be transferred to another person even if that person is using an allowed computing device.

9.6 Mobile Computer Protection

1. Any mobile computer owned by the organization shall at all times operate the following for its own protection:
 - Antivirus program with the latest possible virus updates. The program shall be configured for real time protection, to retrieve updates daily, and to perform an anti-virus or malware scan at least once per day.
 - A firewall program with the latest possible updates. The program shall be operational any time the computer is connected to any untrusted network including the internet to protect the computer from worms and other malware.
 - Additional malware protection software shall be active on the computer in accordance with the anti-virus and malware policy.
 - The operating system and application patch levels must be consistent with the current patch levels of the organization for similar devices and operating systems.

- All mobile computers in the organization shall have wireless access disabled. If wireless access is used, a specific protocol for wireless encryption shall be designated and configured. Also the maximum data sensitivity category shall be noted for the computer depending on the security of the wireless access and other features of the computer.
2. Policy for mobile computers owned by the organization and removed nightly by employees with permission to work from home.
- These computers shall always meet requirement 6.0.1 above.
 - If at any time the computer shall fail to meet the requirement 6.0.1 above, the employee shall report the condition to the IT department and a check of the computer equivalent to any check of an unsecure computer entering the building shall be performed.
 - It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support this process shall not be used in mobile computers. The IT department will determine and specify the proper tools to be used for authentication and access controls.
 - Data to be stored on the computer will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS). The policy must define the encryption tool to use and how it will be maintained.
 - The computer shall be checked weekly by the IT department personnel at designated times when the computer will be entering a secure building area. The check will include a scan for malware and a test to determine whether the computer has a worm. The state of stored sensitive data shall also be checked to determine whether it is encrypted and whether data of too high a level of security is being stored on the computer. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.
3. Policy for computers being used for travel - Protection of these computers shall be the encryption of all sensitive data and a requirement for a valid user ID to operate the computer.

4. These computers shall always meet requirement 6.0.1 above. If any additional software installation is required, it must be done and configured before the computer leaves the building.
5. It shall be ensured that unauthorized persons cannot gain access to the computer without a proper user identification and password. Operating systems that do not safely support this process shall not be used in mobile computers. The IT department will determine and specify the proper tools to be used for authentication and access controls.
6. Data to be stored on the computer during the time the computer is not in a security facility will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS). Any data not considered to be safe to be stored on the computer will be removed using a designated program to be sure it has been removed so it cannot be read using special technology later. There will be a list of documented sensitive data including storage locations for all sensitive data stored on the computer. This list will be created before the computer leaves the facility.
7. If there is a chance that the user will view any sensitive data using their web browser or other program, cached data will need to be encrypted. Cached data that is stored locally such as cached data from the user's browser will be set to be encrypted using the encrypting file system (EFS). This may require Windows XP or some third party software. In Windows XP, this may be enabled using the following procedure:
 - Open "My computer"
 - Click on "Tools" and select "folder Options".
 - Select the "Offline files" tab.
 - Check the box next to "Encrypt offline files to secure data".
 - Click "OK" to exit.
8. If the computer will acquire irreplaceable and valuable data while on the road, the computer user must notify the IT department so arrangements can be made for a method to back the data up.

9.7 Policy for computers being used by contractors

1. The computer will first be checked for compliance with section 6.01 above.
2. The computer will be scanned for malware and tested to determine whether the computer has a worm. Any malware on the computer shall be removed if any was detected. Log information about any malware found.
3. If the computer is in compliance with section 6.01 and contains no malware, the contractor shall report any sensitive data related to the organization that is expected to be stored on the computer.
4. Data to be stored on the computer will be evaluated and rated to consider the sensitivity of the data according to the Data Assessment Process document. Any data stored on the computer that is considered to be sensitive will be stored only in an encrypted format, possibly using an Encrypting File System (EFS).
5. The ID of the computer shall be recorded and it shall be certified for use on the organizational network.
6. The computer shall be checked weekly by IT department personnel at designated times when the computer will be entering a secure building area. The check will include a scan for malware and a test to determine whether the computer has a worm. The state of stored sensitive data shall also be checked to determine whether it is encrypted and whether data of too high a level of security is being stored on the computer. Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly. If the computer is storing data improperly, the certification of the computer shall be reviewed.

9.8 Network Protection

Mobile computers entering the network shall meet the following requirements.

1. If the computer is owned by the Local Government Service and used regularly by employees according to 4.0.2 above, then the computer shall be checked according to that part of the policy.
2. If the computer is owned by the Local Government Service and is returning from a period when an employee used it for travel, the following check shall be performed.
 - Determine whether the anti-virus program is up to date, has the latest virus definitions, is configured properly, and is running properly. If it fails one of

these conditions or has not been scanned for a virus within the last week, a full virus scan must be done before the computer can be used in the building.

- Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
- Test the state of stored sensitive data to be sure it is encrypted.
- Remove any malware on the computer if any was detected. Log information about any malware found. Log any information about data that was not stored properly.

3. If the computer is not owned by the Local Government Service the following must be done.
 1. That organization must agree in writing to allow a malware scan of their computer and agree pay any costs if malware is found on their computer.
 2. A full virus scan must be done.
 3. Test the computer and scan for additional malware such as adware or spyware test to determine whether the computer has a worm.
 4. Remove any malware on the computer if any was detected. Log information about any malware found. The outside organization may be billed for services depending on the assembly's policy.

9.9 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

10.0 NETWORK DOCUMENTATION POLICY

10.1 Overview

This network documentation policy is an internal IT policy and defines the requirements for network documentation in the Local Government Service. This policy defines the level of network documentation required such as documentation of which switch ports connect to what rooms and computers. It defines who will have access to read network documentation and who will have access to change it. It also defines who will be notified when changes are made to the network.

10.2 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to the network.

10.3 Documentation

The network structure and configuration shall be documented and provide the following information:

1. IP addresses of all devices on the network with static IP addresses.
2. Server documentation on all servers as outlined in the "Server Documentation" document.
3. Network drawings showing:
 1. The locations and IP addresses of all hubs, switches, routers, and firewalls on the network.
 2. The various security zones on the network and devices that control access between them.
 3. The locations of every network drop and the associated switch and port on the switch supplying that connection.
 4. The interrelationship between all network devices showing lines running between the network devices.
 5. All subnets on the network and their relationships including the range of IP addresses on all subnets and net mask information.

6. All wide area network (WAN) or metropolitan area network (MAN) information including network devices connecting them and IP addresses of connecting devices.
4. Configuration information on all network devices including:
 1. Switches
 2. Routers
 3. Firewalls
5. Configuration shall include but not be limited to:
 1. IP Address
 2. Net mask
 3. Default gateway
 4. DNS server IP addresses for primary and secondary DNS servers.
 5. Any relevant WINS server information.
6. Network connection information including:
 1. Type of connection to the internet or other WAN/MAN including T1,T3, frame relay.
 2. Provider of internet/WAN/MAN connection and contact information for sales and support.
 3. Configuration information including net mask, network ID, and gateway.
 4. Physical location of where the cabling enters the building and circuit number.
7. DHCP server settings showing:
 1. Range of IP addresses assigned by all DHCP servers on all subnets.
 2. Subnet mask, default gateway, DNS server settings, WINS server settings assigned by all DHCP servers on all subnets.
 3. Lease duration time.

10.4 Access

The IT department staff shall have full access to all network documentation. The IT department staff shall have the ability to read and modify network documentation. Designated IT staff shall have access to read and change network documentation but those not designated with change access cannot change it.

10.5 Change Notification

The staff of the assembly, server administration staff, application developer staff, and IT management shall be notified when network changes are made including.

1. Reboot of a network device including switches, routers, and firewalls.
2. Changes of rules or configuration of a network device including switches, routers, and firewalls.
3. Upgrades to any software on any network device.
4. Additions of any software on any network device.
5. Changes to any servers which perform significant network functions whether configuration or upgrade changes are made. These servers include:
 1. DHCP
 2. DNS
 3. Domain controllers
 4. WINS

Notification shall be through email to designated groups of people.

10.6 Documentation Review

The IT department shall ensure that network documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any network changes were made. Also any current or completed projects affecting network settings should be reviewed to determine whether there were any network changes made to support the project.

10.7 Storage Locations

Network documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

10.8 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

11.0 PASSWORD POLICY

This page provides some basic information that may be included in a password policy. When writing a password policy there is several issues to be considered. There are some experts that argue that password policies in many organizations are too stringent and actually decrease the organization's computer security. When employees are required to change passwords often, meet minimum complexity requirements, and not repeat a password for a minimum amount of time, they may begin to break the rules and start writing passwords down simply because they cannot remember passwords that change so often. The reason for changing passwords is due to the fact that if an attacker gets a hashed or encrypted copy of a password, they can eventually break the password using a brute force attack. This takes a certain amount of computing power and as computers are more powerful, takes less time every year.

However the password policy is setup, it may be worth taking other precautions to protect accounts and passwords. One precaution is not to transmit them on the internet even in encrypted form. Another precaution is to be very careful about network security, to detect any unauthorized sniffing of the internal network, and stringent virus prevention including blocking dangerous email attachments.

Another controversial issue that some experts have discussed deals with the use of passwords versus pass phrases. Some experts contend that passwords are no longer secure and that pass phrases should be used rather than passwords.

11.1 Overview

All employees and personnel that have access to organizational computer systems must adhere to the password policies defined below in order to protect the security of the network, protect data integrity, and protect computer systems.

11.2 Purpose

This policy is designed to protect the organizational resources on the network by requiring strong passwords along with protection of these passwords, and establishing a minimum time between changes to passwords.

11.3 Scope

This policy applies to any and all personnel who have any form of computer account requiring a password on the organizational network including but not limited to a domain account and e-mail account.

11.4 Password Protection

1. Never write passwords down.
2. Never send a password through email.
3. Never include a password in a non-encrypted stored document.
4. Never tell anyone your password.
5. Never reveal your password over the telephone.
6. Never hint at the format of your password.
7. Never reveal or hint at your password on a form on the internet.
8. Never use the "Remember Password" feature of application programs such as Internet Explorer, your email program, or any other program.
9. Never use your corporate or network password on an account over the internet which does not have a secure login where the web browser address starts with https:// rather than http://
10. Report any suspicion of your password being broken to your IT computer security office.
11. If anyone asks for your password, refer them to your IT computer security office.
12. Don't use common acronyms as part of your password.
13. Don't use common words or reverse spelling of words in part of your password.
14. Don't use names of people or places as part of your password.
15. Don't use part of your login name in your password.
16. Don't use parts of numbers easily remembered such as phone numbers, social security numbers, or street addresses.
17. Be careful about letting someone see you type your password.

11.5 Password Requirements (subject to change)

Those setting password requirements must remember that making the password rules too difficult may actually decrease security if users decide the rules are impossible or too difficult to meet. If passwords are changed too often, users may tend to write them down or make their password a variant of an old password which an attacker with the old

password could guess. The following password requirements will be set by the IT security department:

1. Minimum Length - 8 characters recommended
2. Maximum Length - 14 characters
3. Minimum complexity - No dictionary words included. Passwords should use three of four of the following four types of characters:
 1. Lowercase
 2. Uppercase
 3. Numbers
 4. Special characters such as !@#\$%^&*(){}[]
4. Passwords are case sensitive and the user name or login ID is not case sensitive.
5. Password history - Require a number of unique passwords before an old password may be reused. This number should be no less than 24.
6. Maximum password age - 12 months
7. Minimum password age - 3 months
8. Store passwords using reversible encryption - This should not be done without special authorization by the IT department since it would reduce the security of the user's password.
9. Account lockout threshold - 4 failed login attempts
10. Reset account lockout after - The time it takes between bad login attempts before the count of bad login attempts is cleared. The recommended value is 20 minutes. This means if there are three bad attempts in 20 minutes, the account would be locked.
11. Account lockout duration - Some experts recommend that the administrator reset the account lockout so they are aware of possible break in attempts on the network. However this will cause a great deal of additional help desk calls. Therefore depending on the situation, the account lockout should be between 30 minutes and 2 hours.
12. Password protected screen savers should be enabled and should protect the computer within 5 minutes of user inactivity. Computers should not be unattended with the user logged on and no password protected screen saver active. Users should be in the habit of not leaving their computers unlocked. They can press the CTRL-ALT-DEL keys and select "Lock Computer".
13. Rules that apply to passwords apply to passphrases which are used for public/private key authentication.

11.6 Other Considerations

Administrator passwords should be protected very carefully. Administrator accounts should have the minimum access to perform their function. Administrator accounts should not be shared.

11.7 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

12.0 REMOTE ACCESS POLICY

12.1 Overview

This remote access policy defines standards for connecting to the organizational network and security standards for computers that are allowed to connect to the organizational network.

This remote access policy specifies how remote users can connect to the main organizational network and the requirements for each of their systems before they are allowed to connect. This will specify:

1. The anti-virus program remote users must use and how often it must be updated.
2. What personal firewalls they are required to run.
3. Other protection against spyware or other malware.

The remote access policy defines the methods users can use to connect remotely such as dial up or VPN. It will specify how the dial up will work such as whether the system will call the remote user back, and the authentication method. If using VPN, the VPN protocols used will be defined. Methods to deal with attacks should be considered in the design of the VPN system.

12.2 Purpose

This remote access policy is designed to prevent damage to the organizational network or computer systems and to prevent compromise or loss of data.

12.3 Approval

Any remote access using either dial-in, VPN, or any other remote access to the organizational network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

12.4 Remote Computer Requirements

1. The anti-virus product is required to be operating on the computer at all times in real time protection mode.

1. The anti-virus product shall be operated in real time on the computer. The product shall be configured for real time protection.
2. The anti-virus library definitions shall be updated at least once per day.
3. Anti-virus scans shall be done a minimum of once per day.

No one should be able to stop anti-virus definition updates and anti-virus scans except for domain administrators.

2. The computer must be protected by a firewall at all times when it is connected to the internet. Several popular choices include Zone Alarm, the Windows XP firewall, and Norton Personal firewall.

12.5 Remote Connection Requirements

The remote user shall use either dial-In or virtual private networking (VPN). Dial-In is typically used when the user is in a local calling area. VPN is typically used when the user would need to dial a long distance number to connect with a dial-in connection. VPN uses a local connection to an internet service provider (ISP) and creates a tunnel through the local ISP connection to the organizational network. This section specifies the requirements for Dial-In and VPN connections.

12.5.1. Dial-In Requirements

1. Number check - The dial in settings shall be set to perform one or the other of:
 1. Verify Caller ID to a specific number - Use this option if caller ID is available
 2. Always Call back to a specific number - If the user must connect from a location other than their designated location such as their home, they should use VPN.
2. Client Check - A requirement that must be set for Dial-In clients is that a firewall must be installed and operational. If the Dial-In client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
3. Authentication - For authentication of the user, the dial in connection shall use one of:
 1. MS-CHAP version 2
 2. EAP-RADIUS
 3. EAP-TLS
 4. EAP-MD5-Challenge

4. Connection Encryption - This requirement will depend on the data you expect the remote user to be transmitting over the dial-in connection. Typically this should be encrypted especially if the user works for the Finance or Personnel department. The connection shall use one of the following encryption mechanisms:
 1. Microsoft Point to Point Encryption (MPPE)
 2. IPsec

12.5.2. VPN Requirements

1. Client Check - A requirement that must be set for VPN clients is that a firewall must be installed and operational. Also Anti-virus software must be installed and operational. If the VPN client does not meet the criteria, either the connection is not allowed or the client can only access a limited area where they can get the software needed to meet the requirement.
2. The connection choices are PPTP, L2TP, IPsec, and SSL. The connection shall use IPsec which encrypts the data sent through the connection.
3. Authentication - For authentication of the user, the dial in connection shall use Internet Key Exchange (IKE) with digital certificates. The other choice is Internet Key Exchange (IKE) with a pre shared key.

12.6 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

13.0 SERVER DOCUMENTATION POLICY

13.1 Overview

This policy is an internal IT policy and defines the requirements for server documentation. This policy defines the level of server documentation required such as configuration information and services that are running. It defines who will have access to read server documentation and who will have access to change it. It also defines who will be notified when changes are made to the servers.

13.2 Purpose

This policy is designed to provide for network stability by ensuring that network documentation is complete and current. This policy should complement disaster management and recovery by ensuring that documentation is available in the event that systems should need to be rebuilt. This policy will help reduce troubleshooting time by ensuring that appropriate personnel are notified when changes are made to any servers.

13.3 Documentation

For every server on a secure network, there are a list of items that must be documented and reviewed on a regular basis to keep a private network secure. This list of information about every server should be created as servers are added to the network and updated regularly.

1. Server name
2. Server location
3. The function or purpose of the server.
4. Hardware components of the system including the make and model of each part of the system.
5. List of software running on the server including operating system, programs, and services running on the server.
6. Configuration information about how the server is configured including:
 1. Event logging settings
 2. A comprehensive list of services that are running.
 3. Configuration of any security lockdown tool or setting
 4. Account settings
 5. Configuration and settings of software running on the server.
7. Types of data stored on the server.

8. The owners of the data stored on the server.
9. The sensitivity of data stored on the server.
10. Data on the server that should be backed up along with its location.
11. Users or groups with access to data stored on the server.
12. Administrators on the server with a list of rights of each administrator.
13. The authentication process and protocols used for authentication for users of data on the server.
14. The authentication process and protocols used for authentication for administrators on the server.
15. Data encryption requirements.
16. Authentication encryption requirements.
17. List of users accessing data from remote locations and type of media they access data through such as internet or private network.
18. List of administrators administering the server from remote locations and type of media they access the server through such as internet or private network.
19. Intrusion detection and prevention method used on the server.
20. Latest patch to operating system and each service running.
21. Groups or individuals with physical access to the area the server is in and the type of access, such as key or card access.
22. Emergency recovery disk and date of last update.
23. Disaster recovery plan and location of backup data.

13.4 Mail Server Documentation

1. Account size limit where the person receives warnings about mailbox size
2. Account size limit where the person cannot send mail anymore.
3. Account size limit where the person cannot receive mail anymore.

13.5 Access

The IT server administration staff and their management shall have full read and change access to server documentation for the server or servers they are tasked with administering. The IT networking staff, enterprise security staff, application development staff, and help desk staff shall have the ability to read all server documentation.

13.6 Change Notification

The help desk staff, network administration staff, application developer staff, and IT management shall be notified when changes are made to servers. Notification shall be through email to designated groups of people.

13.7 Documentation Review

The network or IT manager shall ensure that server documentation is kept current by performing a monthly review of documentation or designating a staff member to perform a review. The remedy or help desk requests within the last month should be reviewed to help determine whether any server changes were made. Also any current or completed projects affecting server settings should be reviewed to determine whether there were any server changes made to support the project.

13.8 Storage Locations

Server documentation shall be kept either in written form or electronic form in a minimum of two places. It should be kept in two facilities at least two miles apart so that if one facility is destroyed, information from the other facility may be used to help construct the IT infrastructure. Information in both facilities should be updated monthly at the time of the documentation review.

13.9 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

14.0 SERVER MONITORING POLICY

14.1 Overview

This server monitoring policy is an internal IT policy and defines the monitoring of servers in the organization for both security and performance issues.

14.2 Purpose

This policy is designed both to protect the organization against loss of service by providing minimum requirements for monitoring servers. It provides for monitoring servers for file space and performance issues to prevent system failure or loss of service.

14.3 Scope

This policy applies to all production servers and infrastructure support servers including but not limited to the following types of servers:

1. File servers
2. Database servers
3. Mail servers
4. Web servers
5. Application servers
6. Domain controllers
7. FTP servers
8. DNS servers

14.4 Daily Checking

All servers shall be checked manually on a daily basis the following items shall be checked and recorded:

1. The amount of free space on each drive shall be recorded in a server log.
2. The system log shall be checked and any major errors shall be checked and recorded in the server log.
3. Services shall be checked to determine whether any services have failed.
4. The status of backup of files or system information for the server shall be checked daily.

14.5 External Checks

Essential servers shall be checked using either a separate computer from the ones being monitored or a server monitoring service. The external monitoring service shall have the ability to notify multiple IP personnel when a service is found to have failed. Servers to be monitored externally include:

1. The mail server
2. The web server
3. External DNS servers
4. Externally used application servers.
5. Database or file servers supporting externally used application servers or web servers.

14.6 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

15.0 SYSTEM LOCKDOWN POLICY

15.1 Overview

This system lockdown policy is an internal IT policy and defines a general process that should be used to lock down servers and workstations.

15.2 Purpose

This policy is designed to minimize risk to organizational resources and data by establishing a process for increasing the security of servers and workstations by stopping unneeded services and testing for vulnerabilities.

15.3 Server Lockdown and Hardening

This section describes a general process used to lock down servers. When they are initially installed and configured. Types of servers or equipment that need hardening include but are not limited to file sharing servers, email servers, Web servers, FTP servers, DNS servers, DHCP servers, Database servers, Domain controllers, Directory servers, Network devices such as firewalls, routers, and switches.

1. List services that will be required to run on the server. Examples include:
 1. DNS
 2. HTTP
 3. SMTP
 4. POP3
2. List services that are running on the server and turn off any that the administrator is sure are not needed.
3. Do a port scan on the server - Use a security tool to test and determine any ports that the server is responding to.
4. Shut down any services that are not on the required list of services for the server. Especially remember to shut down services listed in Appendix A - Services Recommended for Shutdown.
5. Remove any unnecessary programs, services, and drivers from the server especially those not loaded by default on the server.
6. Patch the server with the latest patches and patch all services running on the server.
7. Disable or change the password of any default accounts on the server or related to any operating services.

8. Be sure all passwords used to access the system or used by services on the system meet minimum requirements including length and complexity parameters.
9. Be sure all users and services have minimum required rights and do not have rights to items not needed.
10. Be sure file share and file permissions are as tight as possible.
11. Perform a vulnerability assessment scan of the server.
12. Patch or fix any vulnerabilities found.
13. Where appropriate, install and run additional security programs such as:
 1. Anti-virus - Install and perform latest update of software and virus definitions.
 2. Firewall
 3. Intrusion detection software - Some approved host based intrusion detection software is recommended to be run on all servers.
 4. Honeypot
 5. Change of system and system files detection

All this software should have the latest updates installed.

14. Set security parameters on all software such as where anti-virus programs will scan, how often it will scan, and how often it will get virus definition updates.
15. Enable audit logging to log any unauthorized access.
16. Perform another vulnerability assessment scan of the server, and fix any discrepancies.
17. Take additional account management security measures including:
 1. Disable the guest account
 2. Rename default administrator accounts
 3. Set accounts for minimum possible access
 4. Be sure all accounts have passwords meeting minimum complexity and length rules.
18. Test the server to be sure all desired services are operating properly.

15.4 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

15.5 Appendix A - Services Recommended for Shutdown

1. File and Printer Sharing for Microsoft Networks - Uninstallation of this service is recommended. This service is not needed unless you want to share a printer on your local computer or share folders on your local computer with other computers.
2. Messenger - Disable this service in the Services applet of Administrative Tools. This service has some serious security bugs and problems and has very little use for managing the network.
3. Remote registry service - This service should be set to manual or disabled since it allows people from remote locations to modify your registry. It is a serious security risk and should only be run if required by network administrators. Set this service to manual or disabled in the Services applet of Administrative Tools.
4. Secondary Logon service - If it is not necessary for lower privileged users to use the "Run As" command to run commands that only administrators or power users can run, this service should be disabled.
5. Universal Plug and Play Device Host service - It broadcasts unnecessary information about the computer running the service. It may be used by MSN messenger. This service is a high security risk and should be disabled unless dependent services are required.
6. Wireless Zero Configuration service - Used to support wireless connections. If you are not using wireless, this should be disabled. This service is a high security risk and should be disabled unless needed.
7. Computer Browser - For home users and most organizational users, this service can be disabled. Running this service is a moderate security risk.
8. NetMeeting Remote Desktop sharing - A person on a remote computer can access your desktop to help you. This service may be used by network administrators to help users with tasks. Normally this service should be disabled unless needed. Running this service is a moderate security risk.
9. Remote Desktop Help Session Manager service - A person on a remote computer can access your desktop to help you. This service may be used by network administrators to help users with tasks. Normally this service should be disabled unless needed. Running this service is a moderate security risk.
10. Network DDE Service - Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers. It allows two running programs to share the same data on the same computer or on different computers. Running this service is a moderate security risk. Normally this service should be disabled unless needed.

11. Network DDE DSDM Service - Manages DDE network shares. Running this service is a moderate security risk. Normally this service should be disabled unless needed.
12. NT LM Security support provider - Used for backward compatibility with older Microsoft operating systems. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual.
13. SSDP Discovery service - Allows the computer to connect with networked plug and play devices on the network. This service does not support internal PnP devices. This service should be disabled unless the computer needs to connect to external networked plug and play devices.
14. Telnet service - The telnet service allows a terminal connection to or from a remote computer but sends passwords in the clear. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual.
15. Terminal services - Allows a remote connection from a remote computer usually used by network administrators to help users. Running this service is a moderate security risk. Normally this service should be disabled unless needed or set to manual. This service is commonly used by system administrators to administer servers remotely.
16. Alerter service - The alerter service allows system administrators to send messages to selected users. This service should be disabled unless specifically needed.

Types of servers that need hardening (This list is not inclusive of all devices that should be hardened):

1. File sharing
2. Email Servers
3. Web servers
4. FTP servers
5. DNS servers
6. DHCP servers
7. Database servers
8. Domain controllers
9. Directory servers
10. Network devices such as firewalls, routers, and switches

16.0 SYSTEM UPDATE POLICY

16.1 Overview

This policy is an internal IT policy which defines how often computer system updates are done and under what conditions they are done.

16.2 Purpose

This policy is required to establish a minimum process for protecting the organizational computers on the network from security vulnerabilities. This policy shall determine how updates are done for both servers and workstations, and who is responsible for performing the updates along with specifying the tools used to perform system updates.

16.3 Update Requirement Determination

This section defines methods used to determine what updates should be done and when they should be applied.

16.3.1 Update Types

Several types of updates may be required on any computer and all the types should be considered for the below listed computer system components. They include:

1. The computer BIOS.
2. The operating system.
3. Application updates.

16.3.2. Update Checking

There are several methods to determine when updates should be performed.

1. Review of posted security flaws and patches for each type of update applicable to the computer system.
2. An automatic scanning of the system to determine available updates not yet applied to the system or application.

The review of posted security flaws and patches should always be used for the computer operating system, BIOS, and applications. The manufacturer website should be used and

there may also be other appropriate sites posting relevant bulletins. If an automatic update ability is available, it should be compared to the listing of posted updates to be sure it is accurate.

16.3.3. Update Vulnerability Types

The update considerations should address vulnerabilities caused by:

1. Code errors
2. Misconfigurations not covered by patches - An example would be a configuration problem with a mail server allowing non authenticated users to relay email using the mail server.

16.3.4. Update Information

Before approving updates, administrators should know:

1. The addressed vulnerability
2. What previous patches are required or what system update is required.
3. What programs are affected by the change
4. What may be broken by the change
5. How to undo the change.
6. It is recommended that new patches be tested in a controlled environment that mimics the infrastructure of the production environment before patches are applied. For assemblies that do not have these resources, one technique is to watch the e - mail groups like NTBugTraq to find out what problems other organizations may be having with the patch. The disadvantage is that you may need to wait a little longer before applying the patch which may slightly increase the time your organization is vulnerable.
7. Be sure you have a good system and data backup before applying a patch on any system.
8. Each server should have documentation including a list of applications running on it and a patch history.
9. All patches approved for client computers or applied to client computers should be documented.

16.3.5. Support Procedures

To support the update requirements definition and update, the following documents should be created to provide a managed response for system updates:

1. A procedure for identifying vulnerabilities, patches, and configuration changes.
2. Procedures for determining how appropriate the patch or configuration change is to each system.
3. Test procedures
4. Prioritization rules
5. Guidelines for implementing patches or configuration changes.

16.4 Server Updates

Server updates shall be done by a qualified and authorized system administrator. Updates for servers shall be checked no less than monthly to determine whether any new updates to any computer system components are required. The system administrator shall determine the following:

1. Whether the update applies to the computer system under consideration.
2. Whether the update is safe to apply or whether it make break an application or some other part of the operating system where functionality is required.

A test environment should be used to determine whether updates may break functionality prior to implementation of production environments. The ability to provide a test environment and thoroughness of determining whether any functionality is broken by the update will vary from assembly to assembly depending on available resources.

16.5 Workstation Updates

Workstation updates may be done using any provided tools depending on the type of workstations and their operating systems. In this policy workstation updates shall be performed using Microsoft system update server. System update server will save a great deal of time and expense since all systems may be updated from one server at the same time. A qualified and authorized system administrator shall review available updates weekly. Normally updates shall be applied in the test environment two to three days before being applied to the main organization.

16.6 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

17.0 USER PRIVILEGE POLICY

17.1 Overview

This user privilege policy is an internal IT policy and defines the privileges various users on the organizational network are allowed to have, specifically defining what groups of users have privileges to install computer programs on their own or other systems. This policy defines the users who have access to and control of sensitive or regulated data.

This policy defines internet access to specific sites for some users or other ways they may or may not use their computer systems.

17.2 Purpose

This policy is designed to minimize risk to Local Government Service resources and data by establishing the privileges of users of data and equipment on the network to the minimum allowable while still allowing users to perform job functions without undue inconvenience.

17.3 Local Computer Privileges

There are three main categories of users on a computer or network. These categories include:

1. Restricted user - Can operate the computer and save documents but can't save system settings.
2. Standard user (power user) - Can change many system settings and install programs that don't affect Windows system files.
3. Administrators - Have complete access to read and write any data on the system and add or remove any programs or change system settings. The majority of users on most common networks should be restricted users on their local computers. Only users with special training or a need for additional access should be allowed to change system settings and install programs that are not operating system programs. This is because many viruses and adware or spyware may be installed in a subtle manner by tricking the user or the installation may be completely transparent to the computer user. If the user does not have the ability to install programs or change settings to a more vulnerable setting, most of these potential security problems can be prevented.

Therefore only users that demonstrate a need and ability for power user or administrator access on local machines shall be permitted to have this level of access. Upon demonstration of a special need for additional access, the IT manager must approve the access before it can be made effective. Groups that may be allowed this type of access include:

1. Domain Administrators
2. Help Desk personnel
3. Application developers for testing purposes who have known computer training or skills.

17.4 Network Privileges

Most network users will have access to the following types of network resources.

1. Email - Most users will have full access to their own email. They will not be able to transfer ownership to someone else.
2. A personal network drive on a networked file server - This is a folder on a drive that only the primary user of this drive can read and write exclusive of domain administrators. The user will not be able to transfer ownership to someone else.
3. A shared group or organizational division's drive - This is a folder that members of specific groups or divisions in the organization may access. Access may be read or write and may vary by organizational requirements.
4. Access to databases - There may be additional databases that may be stored on a shared drive or on some other resource. Most databases will have a standard user level which gives users appropriate permissions to enter data and see report information. However only the database administrators will have full access to all resources on a database. Database administrators will only have full access to the database that they administer.

Groups that may be allowed additional access include:

1. Backup operator - Allowed to read data on the domain for the purpose of saving files to backup media. This group cannot write all data on the domain.
2. Account operator - Can manage and view information about user accounts on the domain.
3. Server operator - Has full privileges on servers including reading and writing of data, installing programs, and changing settings.

4. Domain administrator - Has full privileges on all computers in the domain including servers and workstations. Privileges include reading and writing data, installing programs, and changing settings.

17.5 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

18.0 WIRELESS USE POLICY

18.1 Overview

This wireless use policy defines the use of wireless devices in the Local Government Service and specifies how wireless devices shall be configured when used.

18.2 Purpose

This policy is designed to protect the organizational resources against intrusion by those who would use wireless media to penetrate the network.

18.3 Scope

This policy applies to all wireless devices in use by the Local Government Service or those who connect through a wireless device to any organizational network.

18.4 Risk Assessment

The use of wireless technology has historically been a serious security risk to organizations. This is because it can be an easy access point to gain access to an organizational network. In addition data sent across it may be readable sometimes even when it is encrypted due to some of the vulnerabilities of the encryption schemes used. Therefore this policy requires a risk assessment any time a new type of wireless device is added to the network. Several items must be assessed including:

1. Is this a new technology?
2. Does this device use encryption and if so how well tested is the encryption protocol?
3. What is the cost of implementing a secure encryption protocol?
4. Has this type of device been used on our network before?
5. Can this device be configured to only allow authorized users to access it or the network through it?
6. How easy will it be for an attacker to fool this device into allowing unauthorized access? What methods may be used?
7. What secure authentication schemes are available and what cost or overhead is associated with their implementation and maintenance?
8. How practical is wireless use considering the cost, potential loss, and added convenience?

18.4.1. Authentication

The authentication mechanisms of all approved wireless devices to be used must be examined closely. The authentication mechanism should be used to prevent unauthorized entry into the network. One authentication method shall be chosen. The following must be considered.

1. How secure is the authentication mechanism to be used?
2. How expensive is the authentication mechanism to be used?

18.4.2. Encryption

The encryption mechanisms of all approved wireless devices to be used must be examined closely. The encryption mechanism will be used to protect data from being disclosed as it travels through the air. The following must be considered.

1. How secure is the encryption mechanism?
2. How sensitive is the data traveling through the wireless device?
3. How expensive is the encryption mechanism?

18.5 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

19.0 HUMAN RESOURCES MANAGEMENT INFORMATION SYSTEM POLICY

19.1 Introduction

The overall objective of the Technical Assistance to the Local Government Service Programme in Ghana is to contribute to increased management performance and quality of service delivery, with particular focus on the effective provision of basic services; education, health, water and sanitation at the local level.

A critical part of this Programme is to facilitate a Human Resource Database as a component to support and improve the quality of service delivery in the area of the Human Resource functions and the management of Human Resource information.

19.2 Objective

The objective of developing the Human Resources (HR) Database is to have an improved knowledge-base of human resource data/information strengths, profiles and capacities available within the MMDAs to further plan appropriate interventions in relation to Human Resource Management and Development.

19.3 HR Database System Application

The computerized Human Resources Management Information System has been developed using the computer software program MS-Access as its basic operational means of data processing.

The introduction of the HR Database Application in each of the MMDAs/RCCs is aimed at improving the effectiveness and the efficiency of the delivery of Human Resource Information.

19.4 Responsibilities of the OHLGS, RCCs and MMDAs

19.4.1 Human Resource Management Directorate (HRMD) at OHLGS (Custodians of the HR Data)

- Ensure that new HR Recruits are trained in how to complete the Personal Data Template accurately
- Provide guidance with regards to the HR Data Gathering and Capturing Process
- Assist the RCC with any enquiries and training interventions on Database Management

- Provide a format for standardised reports in consultation with the RCCs
- Play a leading and supporting role in the upgrading of the software by providing input on possible new search criteria.
- Ensure that policies with regards to Data Security are managed and followed

19.4.2. Research Statistics and Information Management Directorate (RSIM) at OHLGS

- Play a leading and supporting role in the development and upgrading of the software
- Provide a detailed IT policy and procedures document that can serve as a strategic guideline to the RCCs
- Provide timely IT support with regards to software or technical problems on the Application when the RCC cannot assist the MMDAs
- Support the RCC to ensure that all IT and HR staff are trained and that continuous follow-ups are done to determine level of competence
- Co-ordinate a six monthly audit on the accuracy of data (sampling processes)
- Ensure Data Security is being applied
- Ensure that all back-ups (follow up on a monthly basis) are submitted and the filing system is kept

19.4.3. Regional Coordinating Councils (RCCs)

- Provide Leadership and Guidance on Database Management in the Regions
- Encourage and Ensure that Assemblies regularly back-up the Personal Database Data
- Follow-up to ensure that the electronic copies are received and the necessary information is also consolidated within the Region before being sent to the OHLGS
- Ensure that RCC's data is always up to date and accurate – set the example
- Manage the Security of Data

19.4.4. Metropolitan, Municipalities and District Assemblies (MMDAs)

- Coordinating Director – provide continuous guidance and leadership to ensure credibility and availability of data.
- Fulfil the role as a change-agent, which would assist with the following:
 - Continuous update of HR Information
 - Arrange and sign –off on information on a monthly basis through a sampling process

- Ensure that IT and HR have the necessary infrastructure (software and hardware) to perform the function
- Utilise standardised HR reports as a decision-making tool
- Ensure that the security of Data are maintained

19.4.5. Information Technology (IT) Officer

- Technical Support to MMDAs
- Ensure that back-up are made according to guidelines.
- Assist with software enquiries
- Manage the security of Data

19.4.6. Human Resource (HR) Staff

- Provide Personal Data Template to new staff members
- Gathering and Capturing of Data
- Ensure all Data is kept up to date
- Verify information and ensure that supporting documents are gathered
- Ensure that supporting documents are available.
- Maintain the security of Data

19.5 Process for the Implementation of the HR Management Database Application

The following processes are envisaged as the specific steps for effective implementation of the HR Management Database Application in the MMDAs;

19.5.1. Determine the readiness of the MMDAs

To facilitate the implementation and support of the HR Database, it will be advantageous and necessary for the MMDAs to provide and make available the following equipment and other associated facilities.

- i) Computer Hardware;** a computer with appropriate memory capability, key board, printer, Uninterrupted Power Supply(UPS), associated connecting cables and back-up facilities

- ii) Computer Software;** Up-to-date operating system (Windows 7 plus), appropriate license agreements for the software programs, installation of the Database application and an appropriate VIRUS protection program

- iii) Office Furnishings/Facilities;** it is essential for good practice for the database processing work routines to be supported within an appropriate secure office

environment, a desk, chair and filing cabinets for securing the Personal Data Templates.

19.5.2. Training for relevant stakeholders

To familiarize the MMDA Staff with the Database Application, it will be necessary for them to be provided with appropriate training;

- i) Assembly Directors/Managers:** to receive an appreciation session on the overall functioning of the Database Application and its potential as a “Management Information Tool”.

- ii) HR Staff:** to receive a number of training sessions on the overall functioning and operational characteristics of the Database Application, Data gathering and transferring data by entering the information into the Database and the use of the Database as a “Management Information Tool” for HR Reports.

- iii) IT Staff:** to receive training sessions on the overall technical functions, operational characteristics and processing abilities of the Database Software Application for maintenance and up-grades.

19.5.3. Personal Data Gathering

To establish and install the database in each of the MMDA locations it will be necessary to capture individual personal data/information from all MMDA employees. To capture this data/information it is necessary to distribute a Personal Database Template for all employees to fill and complete with their appropriate personal information.

19.5.4. Data Capturing

The Personal Data Template will be given to all MMDA/RCC staff (mechanised and non-mechanised) to complete. This process is expected to take approximately two weeks, depending on the number of staff involved in the information gathering process. The distribution process for capturing the data/information is to be organized and managed by the most senior HR Officer at the specific MMDA/RCC.

19.5.5. Verification

On completion of the Personal Data Template the document will be returned to a most senior HR Officer who will check and verify that the template information has been completed correctly. The HR Officer will only accept the personal data template if it has been completed accurately and correctly, validating key

information or when necessary comparing it against key supporting documentation i.e. Education Qualification(s)/Certificate(s) and Social Security National Insurance Trust (SSNIT) Card.

19.5.6 Functional Database Application installed “going live”

The HR Database will “go live” once the following processes are in place;

- The Personal Data Templates have been completed by all MMDA employees and validated by the HR Officer
- The appropriate staff have been given their specialized training on the Database Application
- The Database Application has been installed and is operating effectively in the designated computer
- Pilot run; generating reports and sampling for final verification

19.6 Security

The security of the HR Database and protection of personal data therein is extremely important and all necessary precautions need to be put in place to ensure this.

Some key security points that will have to be considered at the MMDAs;

- i)** The “**Data Protection Act 843, of 2012**” passed by the Parliament of the Republic of Ghana. The Act establishes the protection and privacy of the individual and personal data by regulating the processing of personal information, to provide the process to obtain, hold or disclose personal information and for related matters.
- ii)** The computer and associated supporting equipment are in a secure environment
- iii)** The “hard copy” of Personal Data Templates/files are in a secure environment
- iv)** The “electronic copy” of personal data/files are in a secure environment
- v)** Only authorized persons to have access to the Database application for accessing information/data or entering information/data. Personal Passwords and User Identification(s) will be used as a security mechanism to protect the Database Application and its associated personal data files.

19.7 Conclusion

The primary objective of the HR Management Database is to provide the following

- Standardized and accurate information on personal, educational and job related data of each staff member
- Provide Management Information to assist in making good decisions with regards to HR related functions and processes

19.8 Violation of Policy & Sanctions

In the event of any exceptions to this policy, approval must be sought in advance from the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly.

If it is suspected that this policy is not being adhered to, the incident must be reported to the Head of Service or the Coordinating Director of the Metropolitan, Municipal or District Assembly with immediate effect.

Failure to report any suspected breach of this policy without tangible reason(s) will render the culprit(s) as liable as the person(s) who has been found to have breached this policy.

A person or group of persons found to have violated this policy will be subjected to appropriate disciplinary action which may lead to dismissal or termination of appointment as defined in the conditions of service of the Local Government Service.

20.0 WEBSITE POLICY

20.1 Overview

The objectives of the Policies are:

- To promote best practices to guide the deployment and exploitation of information within the LGS;
 - To ensure data integrity for all users;
 - To ensure the effective and efficient utilization of Information at LGS;
 - To establish standard procedures for the management of the website appropriate to all users.
 - To facilitate the enforcement of standards and best practices to guide the deployment and exploitation of the website within LGS.
 - To monitor and evaluate the effective use of these procedures.
-
- Privacy Policy
 - Links to other sites
 - Third Party Websites and Applications
 - Website Content
 - Information Quality
 - Linking To or Copying Information on the LGS/RCC/MMDA Website
 - Intrusion Detection

20.2 Privacy Policy

20.2.1 Introduction

The privacy policy outlines the information we receive when you visit an LGS site and how we use this information.

The LGS receive two types of information when you visit our site:

- Information automatically collected.
- Information you choose to provide.

20.2.2 Information Automatically Collected

When you visit any website, the site can automatically collect information about your visit. When you browse through our site, read pages there, or download information, we collect certain information to measure how many visitors come to the different parts of the site so we can make the site more useful.

For every visitor, we collect and temporarily store the following information:

- Your computer's Internet Protocol (IP) address, a number automatically assigned to your computer when you go on the Web.
- The domain from which you access the Internet, such as aol.com, you use an America Online account to access the internet.
- The date and time you arrived at our site and how long you spent there.
- The name and version of your computer's operating system and browser, for example Windows/Mozilla Firefox 5.
- The pages you visited.

We use this information to improve our website and provide a better experience for our visitors. We use tools such as Google Analytics etc, to aggregate this information. The information is available only to our Web managers and staff who require this information to perform their duties. It is retained only for as long as needed for analysis purposes.

We use cookies to improve website functions for visitors and to better understand how the public is using our website.

20.2.3 Session Cookies

Some services on our website use "session cookies." These are:

- Small bits of text temporarily stored in your computer.
- Used to aid searching and navigating the site.
- Deleted when you close your browser.

20.2.4 Persistent Cookies

Some services on our website use multi-session cookies, also known as “persistent cookies.” Persistent cookies are:

- Small bits of text temporarily stored in your computer.
- Placed on your computer for more than a single session.
- Used to differentiate between new and returning site visitors, to customize our website for frequent visitors, and to assess site design and content.

20.2.5 How to Opt-Out or Disable Cookies

Both session and persistent cookies pertaining to our website are enabled by default because of their integration with our website. If you do not wish to have session or persistent cookies placed on your computer, you can disable them using your Web browser. If you opt out of cookies, you will still have access to all information and resources at the website. Note: If you disable cookies in your browser, it may cause problems with searching and displaying information.

20.2.6 Information You Choose to Provide

We collect and store no other information about you when you visit our site unless you choose to provide it. For example:

- If you send us an email or submit an online form, we do not automatically receive your email address. However, you will need to provide it to us if you would like an

email response. We will receive no other personally identifying information from your email unless you provide it.

- If you submit a form on our website, we will receive only the personal information you include in the form.
- Children's Privacy: We collect no information from children under thirteen (13). If a child sends us an email inquiry or comment, we will answer it, and then delete the email from our files.

Note: Email is not necessarily secure against interception. If your communication is sensitive, or if it includes personal information such as your social security or staff identification number, you can send it by postal mail instead.

20.2.7 Information Disclosure Policy

LGS will not disclose, give, sell, or transfer any personally identifiable information about our visitors unless it is required:

- By law or regulation.
- For law enforcement reasons.

Other possible uses of your information:

- We may use personally identifiable information to respond to you, in which case various people may need to see the information you provide in order to provide a response to you. If enough questions or comments come in that are the same, your question (but not your name) may be added to our Questions and Answers section. We use this information to help us improve our site.
- We may enter information you send into an electronic database to share
- We may share information with other government agencies that have public health or consumer protection duties, in which case LGS or any of those agencies may contact you.
- In other limited circumstances, including requests from government or private individuals, we may be required by law to disclose information you submit.

20.3 Links to Other Sites

Our website has links to many other government agencies, and, in a few cases, to private organizations. You should be aware that if you access another site through a link we provide, you are subject to the privacy policy of that site.

Reference in any referred (linked) website to commercial products, services, manufacturers, or companies does not constitute an endorsement by the Ghana government, the public services.

LGS is not responsible for the contents of any pages referred from its website.

20.4 Website Content

Any health and medical information on our website is not intended to take the place of advice or treatment from healthcare professionals. It is also not intended to substitute for the users' relationships with their own health care/pharmaceutical providers.

20.5 Information Quality

- Ensuring that all information it publishes reflects a level of quality corresponding to the nature and timeliness of the information.
- Disseminating all its data as broadly and promptly as possible so that the public can benefit from LGS vision of 'A World Class Decentralised and Client Oriented Service'.

20.6 Linking To or Copying Information on the Website

Unless otherwise noted, the contents of the website both text and graphics—are not copyrighted. They are in the public domain and may be republished, reprinted and otherwise used freely by anyone without the need to obtain permission from LGS. Credit to the LGS/RCC/MMDA as the source is appreciated.

If a person, nonetheless, decides to copy content or images, LGS strongly recommends that the copied item lists the date that the material was copied and provides a link back to its source on the LGS/RCC/MMDA website. Users can then see for themselves if the copied material has been updated or changed.

LGS appreciates being informed about the use of website materials.

20.7. Intrusion Detection

This site is maintained by the Ghana Government and protected by various provisions of Data Protection Act. Violations are subject to criminal prosecution in Ghanaian court.

For site security purposes and to ensure that the site remains available to all users, we employ software programs that monitor traffic and identify unauthorized attempts to upload or change information, or otherwise cause damage. In the event of authorized law enforcement investigations, and pursuant to any required legal process, information from these sources may be used to help identify an individual.