دولة فلسطين
وزارة الحكم المحلي

IT POLICIES MANUAL FOR PALESTINIAN LOCAL GOVERNMENT UNITS

2022

دولـــة فلسطيـــن
وزارة الحكم المحلي

IT Policy Manual for Local Government Units

Information Technology Policy Manual for Palestinian Local Government Units

Table of Contents

1 Introduction

The Palestinian Ministry of Local Government is constantly working to develop the work of the Palestinian Local Government Units. In particular, the Ministry of Local Government is working to consolidate current operations, become an advisor on and an executor of the various programme needs, position information technology (IT) within the Local Government Units so that it can effectively be used to improve "Service Delivery," and ensure that IT is capable of expanding into the electronic information age and empowering their transformation into electrified systems.

As a consequence of the Ministry's ongoing monitoring of the state of IT at Local Government Units, it is apparent that they need IT directive policies, which prompted the development of this manual to provide consistent and coherent direction and control (Governance) to follow when they construct their own IT policies based on their specific requirements and without violating any Palestinian national laws. Because national strategies and policies for digital transformation are an essential guiding reference in the preparation of information technology policies at the local level, this manual referred to relevant national policies, including the most recent policy that was approved by the Palestinian Cabinet in 2021: The policy for the information security.

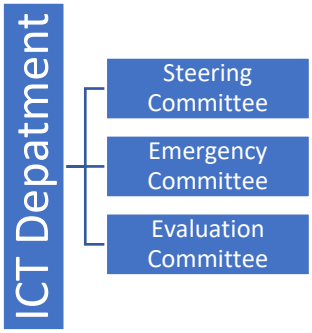
Information Security Standards policy or the identification of Local Government Unit's sensitive information which correlates with the "Information Confidentiality and Information Classification policies" are two policies that clearly intersect with the policies and procedures adopted as general guidelines in this manual. The national "Information Security policy" details a variety of different sub policies that clearly intersect with the policies and procedures adopted as general guidelines in this manual. On another level, the "Risk Management Policy and Access Authority Policy" outlines how to handle and safeguard the information in accordance with the best ways that are globally authorized, as well as how to limit the risk that the information would be lost or corrupted. Methods for storing the information and gaining access to it can be discovered in the document titled "Cloud Computing Security and Use Policy," regardless of whether the information originated from internal or external sources, and by utilizing the policies titled "Encryption Policy, Access Authority policy, Physical and Intra-Physical Security Policy." Last but not least, the "Third Party policy" or the use of external sources helps specify the rights that should be provided or withheld in order to secure sensitive information. It also helps define how to manage the connection with third parties and how to protect equipment and servers.

Naturally, Local Government Units have specific needs that have been addressed in this manual. The purpose of this manual is to consolidate current operations, become an advisor on and an executor of the various programme needs, position information technology within the Local Government Unit in such a way that it can be effectively used to improve "Service Delivery," and

ensure that information technology is capable of transitioning into the electronic information age. As a consequence of this, the Manual's Comptroller will transfer the duty for executing the policies and procedures described in this manual to a competent employee who already has duties within the information technology department.

This manual contains sixteen (16) information technology policies that have been developed to assist the relevant departments in determining the right direction to deal with information security in an integrated manner and in line with international best practises such as the international ISO system. To summarize, the purpose of this manual is to help the relevant departments identify the right direction.

There are three key committees that must be established to build implementation methods, assess performance, and enable decisions on emergency change scenarios, for example specific policy procedures:



Steering Committee: It consists of Officer of the Department, Service Officer, Service Owner, and Procurement Official

Emergency Planning Committee: The members of the Steering Committee are chosen by the Committee.

Evaluation Committee: The officers of the IT department are chosen by the department's top official.

These policies may be changed depending on the demands of the user and what can be applied to the IT systems in use. As a result, because the IT world is constantly changing, the IT department should conduct a periodic review of the policies and procedures in this manual to assess their suitability and applicability, as well as the need to modify them in response to changes in the Local Government Unit or the surrounding environment.

As a result, each local body should review these policies before implementing them, provided that the manual is active as of the date it is adopted by the Local Government Unit. This manual also clarifies the primary duties allocated to the information technology service and the importance of

adhering to these main tasks, so that it may serve as a clear reference in subjects linked to this handbook and the processes for its development, as demonstrated in the sections below:

1.1 Comptroller

The top official in charge of the IT department's policies is known as the "Comptroller." All questions and concerns about this manual's scope and aims should be directed to the manual's Comptroller. The Comptroller of the Manual is responsible for maintaining and distributing the manual in whole or in part, as well as updating and applying it appropriately.

1.2 Breach of Policy

All IT department personnel must follow the rules adopted in this manual after it has been formally authorized by the Local Government Unit, which has the authority to check compliance with this manual on a regular basis. Failure to follow the manual rules may result in disciplinary procedures under Palestinian and Local Government Unit regulations, which may include dismissal of workers and termination of employment ties in the case of contractors or consultants.

1.3 Manual Accessibility

After gaining prior clearance from the manual's Comptroller, the Manual must be made available and accessible to all relevant personnel. The guidebook should be available to all authorities and IT department staff.

1.4 Manual Administration

The comptroller of the manual is in charge of ensuring that the IT management rules and procedures are implemented and followed. The manual comptroller may delegate responsibility for executing the IT management rules and procedures outlined in this manual to an IT department employee with a clear chain of duty.

1.5 Manual Reinforcement

- The manual must function as a dynamic document. Hence every effort will be made to maintain this text up to date including adding new rules and procedures as required. Furthermore, it is envisaged that the incorporated rules and processes would need changes in the future.
- All changes and updates to this manual must adhere to the updating processes outlined in this section.

1.6 The Manual Approval

- The Local Government Unit's council must approve the IT policy and procedure manual before it can be implemented.
- The manual takes effect on the day it is adopted by the Local Government Unit.

1.7 Scope

The IT Department is responsible for the scope of this manual's application, which is overseen directly by its senior officer.

1.8 Maintaining the Manual and Periodic Revisions

To ensure that the manual is up to date and accurate with the most recent actions of the Local Government Unit, it should be reviewed and approved at regular intervals. The following table provides information on the proposed review frequency, who is responsible for audit performance, and who is ultimately responsible for adopting the proposal:

Revision of	Average suggested periodic revisions	Responsible Authority	Approval Responsibility
Policies	Every 12 months	IT Official	General Manager of the Local Government Unit
Procedures	Every 12 months	IT Official	General Manager of the Local Government Unit

1.9 Procedures' Updates

To Examine and Give Approval: The examination and approval procedure are designed to make it possible to conduct an analysis of the "Quality System" to determine whether or not it fulfils the requirements of the Local Government Unit in terms of correctness, technical substance, and comprehensiveness. The fact that the signature blocks have been filled out shows that the document has been examined and authorized by the minimum number of reviewers and approvals required by the document control policy of the Local Government Unit. In addition, the reviewer's signature serves as evidence that they have acknowledged and agreed with the document in its completed form.

Recent developments in Record Monitoring:

- All of the manual's variables need to have a date and a sequence associated with them.
- The date that the information was last updated is written on each page, beside the change number.
- The directory Comptroller ensures that all staff members are familiar with the most recent edition of the manual and any revisions.
- The date when the implementation will begin.

The following schedule must be used and signed to make all updates to the manual.

Document Name		**Document Code**	
Issue Number		**Issue Date**	

Assigned Person	**Prepared by**	**Reviewed by**	**Approved by**
Name:			
Position:			
Signature:			
Date:			

Modifications

Item	**Summary of modification**	**Modification Issue Date**	**Approval**

2 Definitions

2.1 Types of Information Security Threats

1. **System Penetration:** Upon successful penetration of a host computer, data that has been saved may be viewed and altered, and computer processes can be interrupted, changed, or shut down entirely.
2. **Botnets:** one of the most significant challenges facing the Internet in the modern day, and they are connected to the majority of online criminal activities. The majority of malicious activities, including as spam, Distributed Denial of Service (DDOS) assaults, malware, click fraud, and other types of attacks, are caused by botnets and the secretive groups that operate them.
3. **Phishing:** Those who commit fraud flood the internet with unsolicited emails that falsely pretend to come from respectable online retailers or financial institutions. The receiver of the email is encouraged to make changes to their personal profile or complete a transaction by clicking on a link provided in the message. The victim is sent to a bogus website that is made to seem just like the genuine one. However, any personal or financial information that is submitted is sent straight to the individual perpetrating the fraud;
4. **Denial of Service Attack:** An attack known as a "DoS" is one that is designed to completely disable a computer or network, rendering it unavailable to the people for whom it was designed. DoS attacks do this by overloading the target with traffic or by transmitting information that causes the target to crash. The consequence of this for a company that uses that service provider is that the company will not get service until the unwanted traffic has been eliminated;
5. **Identity Theft:** Anyone who uses the internet puts themselves at risk of having their personal information taken from their machines without their knowledge. A hacker or group of hackers may assume the identity of a person who has a genuine account in order to fraudulently gain data or payments.
6. **Theft:** Computer equipment was taken in order to retrieve the data on the hard drive.
7. **Insider:** Fraud committed by workers or other trusted officials, known as insider fraud, which might take the form of unlawful access to restricted data, unapproved administrative activities, or unlawful transactions.
8. **Passive attacks:** Passive attacks are those in which information is gathered but not altered in any way. Taping conversations is an example of a passive attack strategy.
9. **The Active Attack:** Active attacks consist of stealing information and then changing it after it has been stolen. During the transmission process, data fields may undergo modifications such as duplication, insertion, deletion, or alteration.

10. **Social engineering:** Theft of data is accomplished via the use of social engineering, in which the perpetrator poses as a customer or an employee of the Local Government Unit. The caller is successful in persuading the respondent to provide private information to him or her.
11. **Mishaps that are caused by viruses:**
    - **Trojan Horse** - Distributed in conjunction with other software
    - **Worm** is an example of a self-replicating software. The ability to make duplicates of itself. It's common practise to refer to worms that propagate via e-mail address books as viruses.
    - **Logic Bomb-Dormant** is a virus whenever some event activates it (date, user action, random trigger, etc.)
    - **Virus** is self-replicating and does so by attaching itself to other executable files.

2.2 General Definitions

1. **Cyber security:** The means by which the LGU safeguards its networks, computers, and other digital components and the information they hold
2. **Cybercrime law:** The Palestinian Cybercrime Law (No. 10 of 2018).
3. **Deduplication:** It is a mechanism used in full and incremental backups to reduce storage needs by retaining just a single file (one copy) at a given time and date.
4. **Definition of and assistance** with the facilitation of communication between the Local Government Unit and its suppliers in order to ensure the delivery of goods and services in accordance with the plan and within the budget.
5. The "**Department Head**" refers to the Department's Director or an Official who is qualified to participate the "Senior Management Team"
6. **Digital security:** "Digital security" is a catch-all phrase for the measures used to safeguard the information and other IT assets of a Local Government Unit. Antivirus programmes, solid passwords, and a Firewall are all examples of such technologies.
7. **Email:** "Email" refers to electronic communications between people, which may contain text, images, and even additional features like calendars and to-do lists. Whether it's a message transmitted over the LGU's LAN or a dial-up connection to the Internet, this category encompasses it all (ISP). Automatic email distribution to a wide list of recipients is another option (Mailing List).
8. **Electronic Mail Facilities:** Computing Systems/Devices in regard to email enablement, comprising any information technology equipment that links or possibly may connect to the Local Government Unit networks, whether controlled by the Local Government Unit or not; this includes electronic mail facilities.

9. **A Function/process:** A function or process is an activity that, if it stops working, could have a big effect on the way a Local Government Unit works, its reputation, or its ability to make money, as well as on how well it serves its citizens.
10. **Access Control:** The process of controlling how users gain entry to and make use of a system's resources.
11. **Assets:** Assets are things that are valuable to a company because they are helpful in achieving its goals. Equipment, software, data, buildings, and employees are all examples of physical and intangible assets.
12. **Casual Employment:** Temporary or as-needed employment is referred to as "casual employment," and it's used to fill roles that are temporarily vacant or that aren't included on the organization chart.
13. **Change Advisory Board:** To examine and make decisions on Normal Change requests, a group of people called the Change Advisory Board meets.
14. **Change Management:** Upgrading hardware or software on an existing system is an example of a change that must be managed via the Change Management process to guarantee minimal service interruption and continued operation of the company.
15. **Closing a Change Request:** It is an internal administrative process that verifies the desired Change was implemented.
16. **Change:** Any new information or any change to existing information that might have an effect on the LGU's technical services is considered a change. Information technology (IT) infrastructure, applications, systems, procedures, documentation, supplier interfaces, etc. may all need to be updated.
17. **Citizen's Information:** Any file that contains "nonpublic" personal information on a Citizen/customer who gets a service (continuing or terminated) from the Local Government Unit is considered to be "Citizen's Information." Information in any format handled or kept by or on behalf of the Local Government Unit is included here.
18. **Conflict of Interest:** A member of the selection committee or someone else participating in the hiring process has an immediate marital, family, substantial financial, or commercial connection with the individual who is being considered for a job with the Local Government Unit. This conflict of interest may arise from a variety of situations, including but not limited to the following:
19. **Corporate Account:** The Social Media Account Administrator is responsible for creating, managing, and populating the Local Government Unit's principal account on each of the designated Social Media platforms.
20. **Council or Councilor** refers to the governing body of a local government unit or a single elected official serving on such body.
21. **Critical data:** Data that, if destroyed, would have a catastrophic effect on services; examples include financial records and personal information about customers.

22. **Electronic website:** A Local Government Unit's (LGU) electronic website is the location at which data and services are made accessible over the internet at a specific domain name.
23. **Emergency Change Advisory Board:** The Change Advisory Board has delegated responsibility to analyze and make decisions on Emergency Change requests to a subcommittee known as the Emergency Change Advisory Board.
24. To define an **emergency**, we may look at down systems, service disruptions, and unscheduled system restarts as examples. A member of the IT department must authorize any necessary emergency purchases.
25. The term "**employee**" refers to anybody who works for the Local Government Unit, whether under a permanent or temporary contract, and whether they are considered full-time or part-time workers.
26. **Encryption** is defined as the use of an algorithmic procedure with the purpose of transforming data into a form in which there is a low possibility of assigning meaning without the utilization of a secret procedure or key.
27. **Essentials Computer Equipment:** Computers that receive data outside of business hours, network file servers, and networked workstations that backup systems overnight are all crucial pieces of hardware in a well-functioning office.
28. **Entities Outside the Company**: A "third party" is any organization outside of the Local Government Unit that has a service contract with the LGU to perform certain IT management-related responsibilities.
29. **Family member:** A spouse, parent (including step-parent and legal guardian), child (including step-child and legal guardian), sibling, and anybody who resides permanently with a member of Council or an employee all fall within the definition of "family member" under Article 31, Family Members.
30. **FIN Server:** A Financial/Cloud-Based Server
31. **Firewall:** To prevent unwanted access while allowing permitted communications to and from a network or electronic equipment, a firewall examines network traffic based on a set of policy statements.
32. **Hardware:** any component that must have a direct physical connection to a computer or network, such as a computer, monitor, keyboard, modem, memory card, drive unit, printer, cable, etc.
33. **Help Desk:** An organizational unit consisting of personnel, processes, infrastructure, and guidelines
34. **The HR department**, or the IT department's employees, is referred to as "HR."
35. **Incident management:** Incident management often known as ICS or Incident Control and Recovery, is a procedure designed to deal with any unforeseen interruption to a service that has an impact on critical systems and users. with alternatives or fixes, and ensure minimum disruption to regular operations.

36. **Incremental backups:** When you back up your data on a regular basis, you may save time by doing incremental backups after a full backup has already been completed, which only transfer the files that have changed or are new.
37. When you **back up your data** on a regular basis, you may save time by doing incremental backups after a full backup has already been completed, which only transfer the files that have changed or are new.
38. **Information security officer:** A senior member of the IT team whose job it is to protect the confidentiality of LGU data is called an "information security officer."
39. **Information systems:** a network of linked data stores operating under a single set of rules and able to perform similar tasks. Hardware, software, information, data, applications, communications, and people are all common components of a system.
40. **Instant Messaging:** Instant Messaging (often abbreviated as IM or IMING) is a kind of electronic communication that allows users to quickly and easily determine whether or not a specified user is online and, if so, to initiate a conversation with them.
41. **Interoperability:** defined as "the degree to which diverse computer systems, networks, operating systems, and applications can function together efficiently without needing to coordinate their efforts with one another," is the 43rd definition.
42. **"IMIS" (Inventory Management Information System**): a manual or electronic system used to keep track of all of the IT department's physical assets
43. **IT Asset Officer:** In the IT department, an "IT Asset Officer" is the person officially tasked with overseeing all aspects of asset management. Officer of IT Assets is responsible for managing and supporting IT asset contracts within the LGU. To that end, he or she guarantees:
    - The Municipality and its suppliers need to define and improve their communication to ensure that they provide goods and services on time and within budget.
    - Advise upper-level management and employees on IT asset management methods, models, upgrades, and best practises.
44. **IT Infrastructure:** Information Technology Infrastructure (or simply "IT Infrastructure"), which includes all of the systems that make up a company's network, server farm, data storage, and application backend;
45. **IT Officials:** A member of staff who works as an official or the head of the IT department for the LGU.
46. **IT Steering Committee:** A group designated to review requests for policy waivers and other matters pertaining to information technology.
47. **IT:** Information technology
48. **Knowledgebase:** A fundamental component of the helpdesk system, the knowledgebase is a web-based portal that has informational articles, a library for frequently asked questions, solutions to common problems, articles on a particular topic, and a support

section. One of its primary goals is to aid in the education of end users and the expediency with which they may resolve common difficulties that arise while under the care of the support team.

49. **Major and Minor Changes:** A Description of the Levels of Change, as Assessed by Risk and Impact
50. The term "**medium**" refers to any physical medium used to store information, such as a cassette, hard drive, or CD/DVD.
51. **Metadata:** Metadata is information that describes and characterizes other data
52. **The network and systems team** is the group within information technology that is in charge of the design and maintenance of networks and systems.
53. **NIST** is the National Institute of Standards and Technology, which is part of the United States government.
54. **Non-public information:** Any objects, materials, and non-public information (regardless of whether or not they have been converted to paper and regardless of whether or not they are patentable or copyrightable) that are kept private and secret by the Local Government Unit and pertain to either the current or the future business of the Local Government Unit.
55. **Normal:** Any service or system modification that has been requested and is in the pipeline. To be discussed during change management meetings but not executed until thereafter.
56. **Objectionable material:** Pornographic, profane, or sexually explicit content, as well as anything that is offensive to religion or race, fall under the category of "objectionable material," which is defined as "content that defies the values set by the Palestinian laws."
57. An **official record** is any record of information that has been preserved in any form, whether it be in written form or by electronic means, such as official correspondence, an agreement, a memorandum, or a videotape.
58. **Online communication**, sometimes known as "networking," is the process of exchanging information across a digital network, such as the World Wide Web or a mobile phone system (e.g., information sharing, marketing, public engagement).
59. "**Vendors**" providing certain information technology-related services, such as business process Outsourcers.
60. Obtaining services from a third party is known as "**outsourcing**,"
61. **Owner:** A high-ranking member of the team whose function is being outsourced;
62. **Passphrase:** A passphrase is a password-like security measure that is lengthier than the latter for reasons of privacy and/or convenience. You'll often see a mix of capital and lowercase letters, numbers, and punctuation marks in there, and it's usually made up of a phrase or many sentences.
63. **PDC:** Primary Domain Controller
64. **The procedure:** A description of the controls that have to be put into place.

65. **RPO (Recovery Point Objective)** is the maximum quantity of data that may be lost before service can be restored after an outage. The target time until failure is represented as a fraction of the recovery time.
66. A product or service's **recovery time objective (RTO)** is the timeframe in which normal operations may be expected to resume once an event has occurred.
67. **Restoration** entails regaining access to data that has been backed up and resetting it to the state it was in during the backup.
68. **A Risk Management Plan** is a company-wide project that specifies the risky activities, degrees of access, and types of services that an LGU and a vendor have agreed to tolerate. Both the company and the vendor may benefit from the paper, which should describe crucial vendor information.
69. **Risk mitigation** is when an attempt is made to reduce the amount of harm caused by a risk after it has already taken place.
70. **Risk prevention:** the practise of working to eliminate or sidestep potential dangers before they materialize
71. **Risk tolerance:** the readiness to either avoid (prevention) or accept (mitigate) risk
72. **RMF:** Risk Management Framework
73. **Safe Place:** A location with additional safeguards, such as a secured door and visitor records, that is physically separated from the place of origination and use.
74. The term "**security control**" refers to anything done in response to a security danger with the goal of lowering the level of risk. "Precaution" is short for "countermeasure" or "safety precaution."
75. A **security zone** is a collection of interfaces that have been grouped together. To better monitor and categorize data transfer, a network might be divided into "zones."
76. **Senior Management:** In the context of the Local Government Unit, "Senior Management" refers to a group of high-ranking personnel, such as the department heads and the Chief Administrative Officer.
77. **Separate Account:** The Social Media Account Administrator is responsible for creating, managing, and populating all corporate and departmental social media accounts, as well as any accounts created by Local Government Unit councils or committees. Local Government Unit retains ownership of the Account even if employment terminates;
78. **Service Level Agreement (SLA):** An SLA is a portion of a service contract between two parties in which the level of service is officially established for a specific service or system, together with a minimum performance measure over which the service delivery is deemed acceptable.
79. **Service requests:** Requests for new services or solutions, such as more hardware, software, network connection, or access permissions.

80. **Social Media Account Administrator:** An employee who has been appointed by the Local Government Unit to administer a specific corporate or distinct social media account. This person is responsible for authoring and posting material, as well as monitoring, managing, and measuring account activity.
81. **Social media:** a broad category of Internet-based, user-generated content, including websites, blogs, message boards, and social networking services, through which individuals and groups may communicate and share ideas and content. Websites, social media platforms like Twitter, YouTube, Instagram, and LinkedIn, and even blogs and mobile apps all fall under this category.
82. **software patch:** A software patch is an update, correction, enhancement, or extension supplied by the manufacturer for an already existing software product. or upgrade to a newer version of the software, either of which is often deployed by the manufacturer.
83. **Software:** The term "software" refers to any of the several programme packages that are loaded into a computer in order for it to carry out a certain task.
84. **Standard:** A collection of standards that are either system-specific or procedural-specific and must be satisfied by everyone.
85. **Support Requests:** Requests to resolve an issue with an existing service, system, or software, such as a difficulty with network connection or access to a resource or application.
86. **System Change Request:** a detailed request to alter the IT-related systems and infrastructure, which is often made via the "help Desk" and should be completed through the IT Change Management procedure.
87. The "**Helpdesk Division**" is an organizational unit that includes staff personnel as well as operations, rules, and procedures.
88. An **employee** who is employed for a predetermined, continuous length of time with an appointed start and end date, such as a seasonal employee or an employee engaged for a term to replace the leave of a permanent employee. 91. Temporary Employees: An Employee who is employed for a predefined, continuous period of time with an assigned start and end date.
89. **Host name:** One way to tell one device on the internet from another is by its host name, which is its assigned name.
90. A **third party** is defined as an individual or business that provides contracted services to a Local Government Unit.
91. **A transitory record** is one that has no use beyond the accomplishment of a single routine task or is obsolete as soon as it is no longer needed.
92. **Trolling:** Trolling, defined as "the act of creating purposefully insulting or provocative posts with the intent to anger someone, provoke an angry reaction, and/or encourage negative or unproductive conversation," has a prevalence of 95% on the Internet.

93. **Urgent:** Any change that needed to be deployed before the official approval of the change in order to keep Local Government Unit operations and IT services running. 97. Critical: Any change that needed to be deployed before the official approval of the change. Any request deemed an "Emergency" by the IT department must be authorized by the CIO.
94. **Usernames:** Usernames are frequently an abbreviation of the user's full name or an alias, however they may also be referred to as an account name, login ID, nickname, or user ID.
95. "**Vendor Official":** An individual having the knowledge to assess, supervise, and manage the relationship with suppliers is known as a "Vendor Official"
96. **Vendor Risk Management Framework:** The Vendor Risk Management Framework (RRMF) is a methodical and all-encompassing strategy for analyzing present and future dangers and assuring that vendor-related risks are being handled effectively.
97. **Vendor:** An outside provider that sells IT goods, solutions, or services to the LGU.
98. **Windows Server** Update Services (WSUS).

3 IT 16 Manual Policies for Local Government Units

3.1 IT Assets Purchase Policy

3.1.1 Introduction and Goals

3.1.1.1 Policy statement

In order to properly account for the assets utilised by LGUs to access the IT infrastructure, its present state, gaps, and requirements may be analysed with the help of this policy (hardware and software). The IT department/IT Asset officer must be informed of any changes in ownership, allocation, configuration, or use of these assets that occur off-site from the Local Government Unit's offices.

3.1.1.2 Purpose of the Policy

In order to make sure that the IT department or IT officer is keeping an eye on everything that has to be protected from a security standpoint, it is important to create a list of everything that belongs to the Local Government Unit that relates to information technology.

3.1.1.3 Scope Of the Policy

Regardless matter where in the world they may be located, this policy applies to all employees (including full- and part-time), suppliers, business partners, contractor people, and functional units who make use of the IT-related assets of the Local Government Unit. This Policy extends to any third-party-operated or contracted-for Local Government Unit Information Systems environment. In search of innovative answers (hardware and software)

3.1.1.4 Responsibilities of the Policy

- The principal point of contact and the person accountable for ensuring that this policy is put into action is an official in the IT department.
- The Asset Management Department (financial department) will work with the Information Technology Department to create and maintain an inventory of all IT assets.
- Third, everyone in the Local Government Unit—from the mayor down to the lowest-level employee and contractor—must do their share to guarantee that every asset is accounted for.
- The IT Department is solely accountable for ensuring the security of all IT-related systems and data within the LGU.
- The IT committee formed by the Local Government Unit or the Council should evaluate this policy annually and make any required adjustments.
- Risks connected with using the IT assets and infrastructure of the Local Government Unit should be communicated to all personnel.

3.1.2 Policy and Procedures

1. You'll want to catalogue your most important IT resources. Among the most important resources are:
    i. Components that link together a network (routers, switches, hubs etc.)
    ii. Servers (mail, file, web etc.)
    iii. External connecting components (modems)
    iv. Components of security (authentication servers, firewalls)
    v. Personal computers and portable electronic devices.
2. The Inventory Management Information System (IMIS) shall include complete and accurate records of the Local Government Unit's essential IT assets, including but not limited to the following:

    a. Identifying each asset individually is essential for every IT system. The identifying method employed here must guarantee the following: The identifying method employed here must guarantee the following:
        - Knowledge of the physical location of the IT assets.

- Second, we know who provided the IT asset (supplier information must be available).
- The identification of IT asset maintenance contracts.
- The people answerable for the property are identified.
- The final six digits must be numbers to meet the requirements of the Naming Convention Policy, and so on.

b. **Description:** very important piece of IT infrastructure should have a brief explanation accessible. Information technology assets should be described in broad terms, including their primary purpose and usage, as well as their current state (whether "stock," "operational," "under repair," or "disposable"). Usefulness, monetary worth, useful life, and asset kind are all factors that might inform an optimal asset disposal strategy.

c. **Configuration:** Every crucial IT asset should have configuration details readily accessible. It is important to include both business needs and technical configuration documents when discussing an IT asset.

- **Linkages (where appropriate):** As needed, you should also provide Connections, which is data on how this resource connects to other crucial IT assets.
  1) **Model and type:** the model and type of the IT asset
  2) **Serial number:** the serial number of the IT asset
  3) **Identification:** a unique identification number (where relevant)
  4) **Location:** the location of the IT asset;
  5) **Supplier:** the supplier's name.

Clarification: The above is required for all mission-critical IT assets and strongly recommended for all other IT assets.

A. First Evaluation (internal)

Once all IT-related assets have been documented, the next stage is to assess the department's preparedness to provide the requested services to the Local Government Unit in light of other Policies, such as the Risk Management Policy. What is their present state as determined by a set of "minimum Operational Standards" of Fundamentals of an IT system comprised of five

categorized themes to evaluate the infrastructure (see appendix 1) and respond the LGU absolutely requires in order to carry out daily tasks?

- Internet Connection
- Anti-Virus (Licensed) on all computers
- Up to date vendor supported Software
- File Backup
- Strong passwords to enable data protection

B. Gap Analysis

The IT team should use the results of the initial assessment to conduct a Gap analysis and come up with areas for improvement and potential solutions or an approach to address deficiencies, create inventory documents like stock requisitions, stock transfer receipts, stock returns, or manage any identified obsolete pieces of equipment. As an instance, if you test your Internet connection, you can find out that your network is lacking in some way, perhaps because you don't have a firewall or enough network switches. Departmental difficulties, such as unsecured public Wi-Fi and the internet, and the need to increase security via stronger passwords are two examples of what may cause a void.

C. Budgeting and Decision-Making Procedure

Based on the results of the Gap analysis, an IT strategy for the next # years will be developed. The IT department's job is to keep track of how much money is needed for new computer gear and software, compare it to the authorized IT plan, and make any necessary recommendations for funding, whether that comes from the operating or capital budget. It is recommended that the IT department use Appendix 2 as a guide for implementing the approved plans. The council should be presented with the plan in order to study, approve, and incorporate it into the requisite funding proposals.

D. Service contract

The yearly maintenance contract value must not exceed 10% of the initial contract buy value, which is why this condition should be included in all IT equipment and software purchase contracts.

E. IT Asset Retirement and Disposal

The IT department is responsible for creating and maintaining a protocol for getting rid of old IT equipment. This process should include steps like inventorying equipment, determining its value, getting the necessary approvals, and finally, getting rid of the old equipment. In order to safeguard

sensitive "unpublic" information, all recognized (in the IMIS) obsolete computer equipment must be disposed of in accordance with predetermined security protocols. The IT department and the Asset department or the Finance department of the Local Government Unit must approve a "Request for Disposal" form before it can be used to document the disposal of any assets.

3.1.3 Related Policies

1. Disaster Recover Policy
2. Risk Assessment Policy
3. Backup Policy

3.2 IT Risk Management Policy

3.2.1 Introduction and Goals

3.2.1.1 Policy Statement

The goal of this policy is to establish a framework for analyzing, assessing, and mitigating risks by identifying and assessing potential vulnerabilities and threats in the IT environment of the Local Government Unit, as well as to provide guidelines and standards for managing all IT Risk management matters pertaining to the Information Technology of the Local Government Unit. The plan's objective is to deal with these risks and include offered solutions that are consistent with supported policies including the Backup Policy, the Disaster Recovery Policy, and the Information Security Policy.

3.2.1.2 Scope

This Information Technology Risk Management Policy applies to all of the municipal technical and communications infrastructure and equipment that is managed by the Information Technology

Services, as well as all of the users of municipal technical devices. It also applies to any third-party subcontracted services that may be used.

3.2.1.3 Purpose

This IT Management Policy Risk provides the Local Government Unit with instruments to help it successfully manage risk by determining what dangers exist in its IT infrastructure, ranking those threats by severity, and settling on countermeasures. Applying this policy helps in achieving:

- Verify that the Local Government Unit is taking an "appropriate" amount of risk in its operations;
- Allow the Local Government Unit to develop a primary framework for Risk evaluation;
- Third, put safeguards in place to prevent the risk from happening and/or lessen its impact if it does.
- Data Protection, Backup and Recovery, and Data Security should be pre-established in the (**Disaster Recovery Policy**) to provide minimal disruption to business operations in the event of a disaster.

3.2.1.4 Responsibilities

- Keeping this policy updated is the job of the IT department's top administrator.
- The IT Steering Committee or council of the Local Government Unit must annually evaluate the policy and approve any revisions.

3.2.2 Procedures and Policies

3.2.2.1 Policy

1) The IT Department is responsible for safeguarding and maintaining full control of all electronic systems used by the Local Government Unit, including those used in connection with any third parties.
2) Construct a scheme for identifying threats to the Local Government Unit's operations and its capacity to deliver services to its constituents (the Risk Management Framework "RMF" adopted by the U.S. government's National Institute of Standards and Technology is described in this manual as an example scheme the Local Government Unit can adopt).
3) Furthermore, establish goals for the context, establish criteria for each risk and how to evaluate it, and provide a context for IT risk assessment that includes both internal and external threats.
4) Define risks in line with the needs of the LGU's activity, do an analysis of each kind of risk, and follow the appropriate processes to establish common controls against all threats

in order to prevent the risk from occurring and/or lessen its impact once it has already been exposed.

5) Draft a Critical Infrastructure Protection (CIP) plan, outlining the assets' dependencies on one another, the resources available to deal with the threat, and the people who can lend a hand, as well as how the situation will be handled in terms of damage control, system isolation, and data recovery.
6) Data Protection, Backup and Recovery, and Data Security should be pre-established in the (Disaster Recovery Policy) to provide for little disruption in the event of a disaster.
7) The Service has identified possible dangers, and all staff members need to be made aware of them so that they may be prepared.
8) Repeat this process of review on a regular basis (at least once a year) to keep track of any changes and to spot any potential dangers or weaknesses.

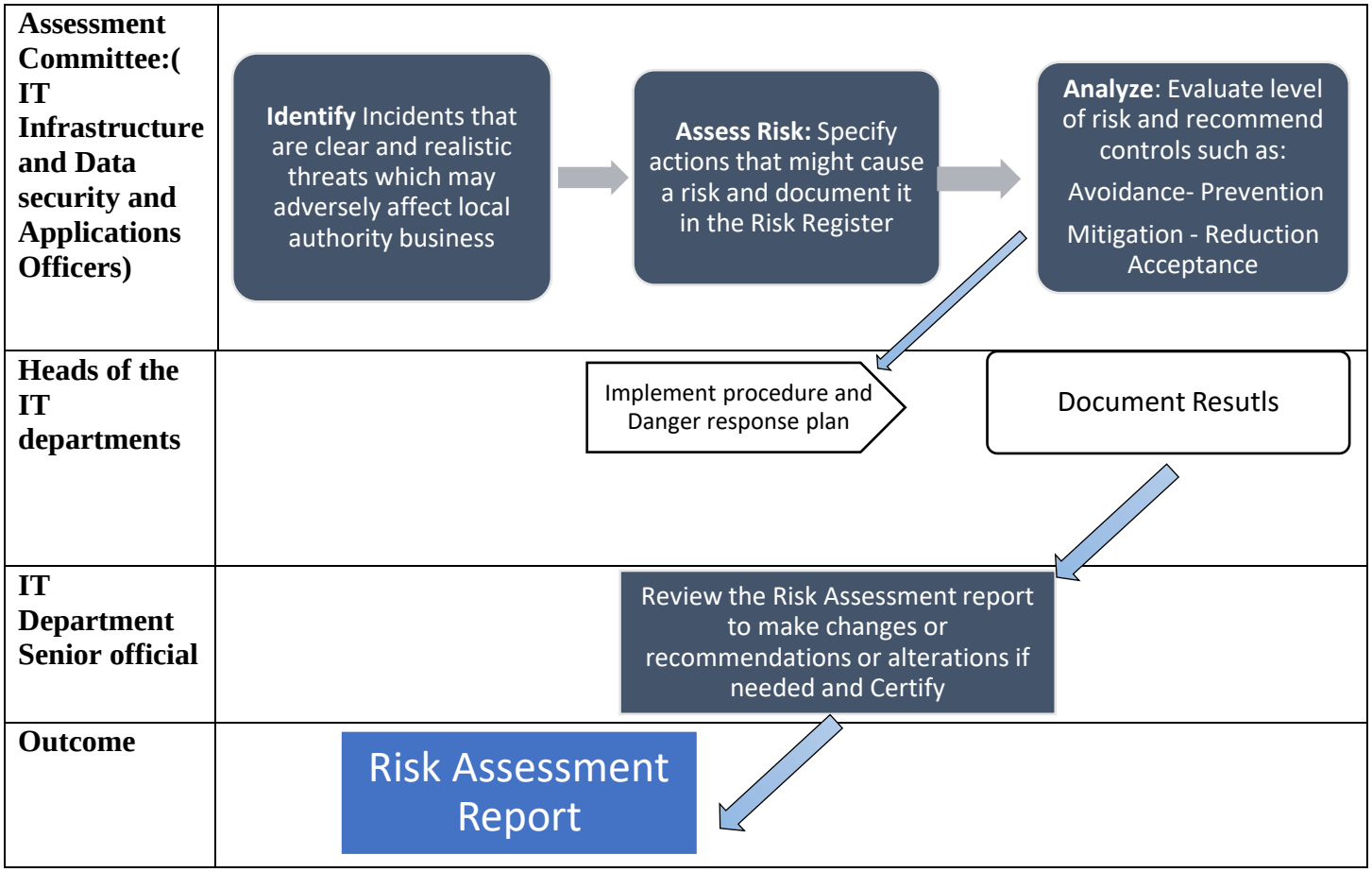
3.2.2.2 Risk Management Plan procedures

The risk management plan is a process responsible for identifying, assessing and controlling risks.

Number	Responsible Individual	Process	Time	Procedure	Output
1	**Assessment Committee:(IT Infrastructure and Data security and Applications officers)**	**Identify** Incidents that are clear and realistic threats which may adversely affect Local Government Unit's business			Incidents Register
2	**Assessment Committee**	**Assess Risk:** Specify risks that might cause a risk and document it in the Risk Register			Risk Register

3	**Assessment Committee**	**Analyze**: Evaluate level of risk and recommend controls such as: 1. Avoidance-Prevention 2. Mitigation & Reduction 3. Acceptance			No output
4	**Heads of the IT departments**	Implement procedure and response plan to risk and document results			No output
5	**IT Department Head Official**	Review the Risk Assessment report to make changes or recommendations or alterations if needed			Risk Assessment Report

3.2.2.3 Risk Assessment work cycle



3.2.3 Related Policies

1. Disaster Recovery Policy
2. Password Change Policy
3. IT Backup Policy
4. IT Outsourcing Policy
5. Digital Security Policy

3.2.4 The Risk Management Framework “RMF”

Several worldwide methodologies exist for constructing the "RMF" risk management framework, and many of them have similarities with the "NIST" Cybersecurity Framework, as briefly stated in the following section.

The NIST framework comprises seven fundamental steps: Prepare, Classify, Select, Implement, Evaluate, Authorize, and Oversee:

- Even if the Local Government Unit systems are already operational, the preparation is a prerequisite for completing the next processes. The Prepare stage seeks to provide the Local Government Unit with proper risk-related preparations. In this stage, key risk management roles are identified, and the risk management strategy establishes which "important" data requires backup systems and corresponding recovery information needs, as well as any redundancies required to ensure the safety and integrity of the data in order to feed the Disaster Recovery Policy. In addition, at this point the Local Government Unit must define and identify its risk tolerance, which is often related with the allocated budget. Risk tolerance is a mix of the relative relevance of data in the infrastructure and the capacity to recover in an acceptable amount of time using existing procedures. This information should be included into the risk management plan, and the associated procedures and processes should be recorded in order to facilitate yearly assessment.
- The second stage is to "Categorize" the system effect of the risk. The goal is to record the system's characteristics and security for senior IT authority approval.
- The third stage is to "Select" the appropriate controls to safeguard the system in the Local Government Unit that has been identified as system-specific, hybrid, or common. The fourth stage is to implement the controls to ensure that they are also current and represented in the Security and privacy plans.
- The objective of the fifth step, Assess, is to develop a plan of action and milestones based on the findings of the implementation stage about the controls selected and whether they were implemented properly and are functioning as intended to provide the desired security and privacy objectives.
- The sixth stage, Authorize, grants permissions for the system controls and risk responses defined by the IT official. The last stage, Monitor, maintains a continuous monitoring schedule based on an authorized "monitoring strategy created in the Prepare step," and the output of this step supports risk management choices.

3.3 Disaster Recovery Policy

3.3.1 Introduction and Goals

3.3.1.1 Policy Statement

This policy is intended to advise and help the Local Government Unit in maintaining the effective management of electronic data retrieval and in enabling data recovery in the event of system disc driver failures, data input mistakes, or natural catastrophes. It is recognized as a critical component of the functional operations and IT systems of the Local Government Unit. The documentation of these processes is required as part of the system implementation.

3.3.1.2 Scope

The policy primarily applies to the IT department responsible for protecting the IT systems of the Local Government Unit.

3.3.1.3 Purpose

This policy's implementation helps to:

- Permit the Local Government Unit to create alternate ways of operating with little disruption in advance.
- Protect the confidentiality and integrity of information inside the IT systems and minimize the degree of any potential damages.
- Utilizing a restoration method, ensure "Business Continuity" via the prompt usage of important data.
- Reduce enterprise and legal risk
- To instruct workers in emergency measures
- To ensure the seamless and speedy resumption of service

3.3.1.4 Responsibilities

- A member of the IT Department is responsible for overseeing the execution of this policy.
- The "Steering Committee" will appoint an "Emergency Team" to execute the recovery.
- The sole Local Government Unit department responsible for the security of IT systems and data is the IT department.

- The General Manager of the Local Government Unit is in charge of the business continuity programme, and the department heads are responsible for determining the RTO and RPO based on the criticality and effect of the business operations.
- The IT department is responsible for establishing IT recovery strategies that allow the firm to meet its RTO and RPO.
- The IT department is responsible for handling all internal and external communications necessary for the continuation and recovery of IT services.

3.3.2 Procedures and Policies

3.3.2.1 Policies

1) The Local Government Unit is required to create its own recovery controls and processes.
2) The IT department must design a pre-defined alternative operating mode with minimum downtime, defining the recovery time objective and the recovery point target as specified below:

RTO & RPO

a) The recovery time goal "RTO" and recovery point objective "RPO" are components of the Business continuity plan (BCP), which outlines the specific catastrophe risks, preventive measures, and recovery solution for the Local Government Unit.
b) The RTO addresses the question "how fast might operations be resumed after a major event?" During the Business Impact Analysis, the owner of a process establishes the starting point for assessing what sort of disruption the Local Government Unit can sustain and what activities must be done to reach those recovery time targets. Included in viable strategy alternatives would be any efforts that would permit the restart of a business process at or near the RTO. The RTOs are then offered for approval to higher management.
c) Recovery point target the "RPO" metric is used to estimate the optimal recovery point for data backups. Therefore, if the IT department determines that a data loss of more than # hours will result in unacceptable losses or other negative effects on operations, then the backup recovery points should not exceed # hours. For instance: Twelve hours of data not included in the most recent backup

3) Systems must be implemented to preserve the confidentiality and integrity of information and to mitigate any harm.

4) Continuity of business must be assured by using vital data immediately throughout the recovery phase.

5) Provide a recovery control method that strikes a compromise between assuring best practise controls and service efficiency based on system needs, vendor recommendations, and strict adherence to the Data Backup policy's processes.

6) All workers must be educated in emergency measures to ensure a swift and seamless service restoration.

3.3.2.2 Recovery Procedures

For systems supported by the vendor, adhere to all vendor requirements. For internal servers and systems, carry out the following procedures:

- The IT department determines the IT recovery priorities based on the RTO and RPO established by the business department and formally authorized by senior management.
- Determine the IT recovery order based on the relevance of the activities outlined in the plan: which servers, workstations, email, etc. will be activated first.
- Delete the affected files and restore the most recent "clean" backup if data has been compromised.
- If application software has been compromised, remove all programme files and reinstall it using the vendor's original installation media.
- If operating systems, security, or both. If telecommunications software has been hacked and time is of the essence, install the backup server and software quickly to enable time to "clean" the system, reinstall and test all applications and software on the original system, and "reload" the system.

The restoration process documentation must include the following:

- Identification of crucial data and applications
- Documentation and support materials needed to the Local Government Unit's execution of critical recovery activities.
- Recovery procedures are described in the third section.
- Provision for key management in the event that data is encrypted.

3.3.2.3 Restoration Procedure Testing

1) The operational staff, under the direction of the IT official and with the assistance of the Emergency team, is responsible for testing system software and data backups on a regular basis by restoring a sample of the backups according to a formal schedule in the test environment to ensure that it does not affect the production environment.
2) According to the IT Backup Policy, the IT Official is responsible for regulating and overseeing backup testing.
3) Regularly test the Restoration processes (at least once per month) to verify that they are effective and can be finished within the timeframe specified in the operating procedures for recovery.
4) **Ensure Accessibility:** The real amount of time necessary to restore the data.
5) Maintain documentation of the backup restorations
6) Incorporate internal and external Communication strategies.

3.3.3 Related Policies

- Risk Management policy
- IT Backup policy
- IT Assets Purchase policy

3.4 Change Management Policy

3.4.1 Introduction and Goals

3.4.1.1 Statement of Policy

The policy's goal is to guarantee that any changes made to the operational environment's information systems, IT infrastructure, and applications are always properly identified, authorized, tested, approved, implemented, and documented, thereby minimizing the likelihood of interruptions or shutdowns.

3.4.1.2 Scope of the Policy

Information Technology (IT) systems and infrastructure administered by the IT department or outsourced to a third party, or receiving technical assistance, are within the purview of this policy.

3.4.1.3 Purpose of the policy

- One goal of Change Management is to minimize the potential for harm caused by Changes.
- Modifying IT infrastructure with fewer mistakes
- Make adjustments with as little impact as possible on IT services
- Lastly, it sets out detailed standards and processes to guarantee the continuation of services to people and the protection of information in the event of an emergency or routine adjustments to IT systems and infrastructures.

3.4.1.4 Responsibilities and Roles

- The person in charge of IT or his designated agent must put this policy into action.
- In step 2, the IT Official will convene a Change Management Advisory Board consisting of the heads of the various IT units, the head of the requesting unit, and any other person considered appropriate to participate, who will have final decision-making power over the proposed modifications and will follow the processes outlined in this policy.
- Upon receiving a request for a change, the IT Official will convene an Emergency Change Management Advisory Board consisting of the head of the technical support unit

and any other individuals deemed necessary to participate who will have final decision-making authority over the request in accordance with the procedures outlined in this policy.

- If the Committee can't agree on whether or not an emergency update to the system should be made, the IT department head or his or her designated representative will make the call.
- Furthermore, if there is an issue with the functioning of the IT systems or the delivery of services, workers and independent contractors are obligated to notify it.
- To discuss scheduling problems and assess System Change Requests (Appendix 5), the Designated Change Management Board will meet.
- Predictable downtime It is the responsibility of the GM to approve any change request that will have an effect on LGUs during business hours, regardless of its length.
- High-impact requests for changes to the System must be approved or rejected by the General Manager of the relevant Local Government Unit or his authorized representative.
- The Local Government Unit is free to adjust the meeting schedule as it sees fit.

3.4.2 Policy and Procedures

3.4.2.1 Policies

1) The LGU must implement a system of formal management and control over any modifications to its information systems and IT infrastructure.
2) Here are some criteria by which modifications may be categorized:

Changes should be classified according to the following:

a. **Normal change:** Changes (whether major or minor) are planned, studied and approved prior to the change and documented.
b. **Standard change:** a change that is restricted to standard and/or regular work effort (already authorized), which may not need a formal change request or a test plan, but should be recorded to offer an audit trail. For post-hoc administrative changes to take effect, they need to be approved by the relevant department's Official.
c. Time is of the essence, and these adjustments must be made as soon as possible, thus they take precedence over the "Normal Changes" that had been planned. Please go to the Help Desk Procedures for more.

3) It is important to record, assess, and approve proposed changes before putting them into action, and then compare the actual outcomes to those that were anticipated beforehand.

4) The IT department executes all "Normal Changes" in accordance with the change management processes outlined in this policy.

5) The IT team has to consider how new developments can affect data protection and security.

6) Because this change may have an effect on the operations of other departments, the IT department must determine which systems are potentially impacted and tell the appropriate parties accordingly.

7) Before beginning the process of making the adjustments, it is necessary to secure the necessary authorization from the IT official.

8) To ensure that only authorized individuals are able to make changes to the configurations of systems that store or transmit information,

9) The Emergency Changes protocol should be followed in a timely and efficient manner to make any necessary adjustments in the event of an emergency.

10) When an emergency occurs, the change request must be processed and closed just as a regular change request would be.

11) The department head who would be impacted by the suggested adjustments should be kept up to date on their progress (see Help Desk Policy).

12) The Helpdesk keeps a separate log to track and record any and all changes to the IT infrastructure and systems (see Helpdesk policy).

3.4.2.2 Priority Status

ITIL uses three metrics for determining the order in which incidents are processed (unorganized interruption or stop in service) and specify the status of change:

1. Impact - The effect on business that an incident has

a) High : interruption to critical business processes
b) Normal : interruption to the work of individual employees

c) Low :hindrance to the work of individual employees, continuation of work possible by means of a circumventive solution)

2. Urgency - The extent to which the incident's resolution can bear delay or (available time until the resolution of the Incident) for example.

a) 1: to 0.5 hrs.
b) 2: to 2.0 hrs.
c) 3: to 6.0 hrs.

3. Priority - How quickly the service desk should address the incident, and (as a suggestion): the Priority values are defined as follows:

a) Priority 1 = low = 16hrs
b) Priority 2 = normal = 8hrs
c) Priority 3 = medium = 4hrs
d) Priority 4 = Critical = 2hrs

ITIL suggests that priority be made dependent on Impact and Urgency according to the following table:

	URGENCY 1	**URGENCY 2**
IMPACT 1	PRIORITY 1	**PRIORITY2**
IMPACT 2	**PRIORITY 2**	**PRIORITY 3**
IMPACT 3	PRIORITY 3	**PRIORITY 4**

Please note that the Expected Resolution Time should be estimated by the IT department, taking into consideration that the incident may require involvement of external parties.

3.4.2.3 Procedures

Submittal of a Normal Change request:

The "Help Desk" submits a Change request which should document information about the required changes with a full explanation of its reasons, which could be such as:

1. An accident that led to a new change.
2. Change as a result of a known issue.
3. The End User requests a change.
4. The department Official or his representative requests a change as part of the ongoing maintenance.

The Helpdesk -as first line of support- will route the Change requests to designated IT personnel or the service\system suppliers to be studied and evaluated, and then sent to authorized personnel for approval. The change request should be submitted according to:

1. Planned requests must be submitted no less than (# business days).
2. Planned request that requires a security evaluation must be submitted not less than (# business days).

3.4.2.4 The Normal change processes

1. **Plan**: Determine the reasons for the change, implementation design, the functions and divisions affected by the change, communication plan, test plan, backout plan (if needed), schedule and the desired result of the change.
2. **Evaluate**: Determine the impact of the change and potential risks in priority level of service and the nature of the proposed change, (please check the Risk Assessment Policy); determine the change type and the change process to use. Determine the estimated costs of making the change, estimating the benefits to the Local Government Unit, and documenting the information.
3. **Review**: Discus with peers and/ or Change Board as appropriate.
4. **Approve**: All Change requests must obtain necessary approvals from the head of the department submitting the request and then the Advisory Board Committee.
5. If Change request is "Denied", requester will be informed with reasons (e.g. scheduling conflicts, resource issues, etc.);
6. If Change request is approved, execution of the change shall follow internationally accepted project management standards so that all constraints (e.g. time, cost, scope etc.) are factored into the design of the activity. The following process will start:

a) Prioritize actions in the change request to allocate key resources.
b) Setting a timetable for implementation.

7. **Communicate**: Identification of departments that may be affected by the change in order to inform them of the latest developments; Document the Change and inform the requester. (See Helpdesk policy);
8. **Implement**: When the order is issued to the roll-out team (who is responsible for the change), a plan is made of specific activities for implementation including the timeline and the method, and/or a purchase order is made for the technical items needed for implementation (See IT asset purchase policy);

a) The team responsible for the implementation will examine the required changes in the testing environment using appropriate tools, and develop a plan to Backout the approved changes as required in the Information Security Policy and Disaster Recovery Policy if the change fails.

b) Before starting the implementation in the operational environment, all relevant departments that may be affected by the change should be notified.
c) When implementing changes in the operational environment, appropriate times must be chosen to make changes that minimize interruptions to IT services.

9. **Document**: Document the change and any review approval information

3.4.2.5 Emergency Change request

1. If the change request is an "Emergency", it must be referred immediately to Emergency Commission to track and to study and evaluate the request based on the available data to reach a clear opinion: approve or reject the request;
2. A Helpdesk Major Incident Report Form is required for tracking purposes. Any exceptions to this process must be justified with and approved by the Requester's official.
3. If the Change request approved, an immediate implementation of the plan for urgent changes to contain emergency situations can be started without going through the detailed procedures for the "Normal Change" request;
4. After the emergency situation is contained, the IT Official or his/her representative makes an assessment of the emergency changes that have been made to make a decision either to keep the changes permanently or make additional modifications and improvements to them with documenting the changes in the change register.
5. A Backout Plan should be prepared if the decision to make additional modifications.

3.4.2.6 Post Change Follow-Up

After the change has been implemented and tested, the following applies:

1. The IT department official and the head of the roll- up team will review all changes and update the status of the successfully implemented changes as "Successful -Closed" and document the changes in the record. This applies only to Normal and Emergency changes.
2. The Helpdesk will inform the requester and verify with the Requester/ Owner the results;
3. The Helpdesk will update the Change Request Log and file all documents;
4. The Helpdesk will send informational emails notifications, general notifications, scheduled changes, rescheduled changes according to the Helpdesk policy.
5. The requester is notified that the change request is "Closed".
6. IT must evaluate the technical feasibility of the change and the whole impact of the change in terms of:

a) Performance
b) Capacity
c) Security

3.4.3 Changes verification

Helpdesk will verify with the Business unit/ requester the implemented change against the following entries:

1. Protocol of actions
2. Person in charge
3. Support Group
4. Time and Date
5. Description of the activity
6. Documentation of applied workarounds
7. Documentation of the root cause of the Service interruption
8. Date of the Incident resolution
9. Date of the Incident closure
10. Specify results post change

3.4.4 Helpdesk Role

1. The “Helpdesk “will follow procedures stipulated in Helpdesk Policy to document requests, inform requesters and other affected departments, and track Changes status.
2. The “Helpdesk” will document the Change Committee’s meeting minutes for future reference.
3. The Helpdesk will log requests onto the Change Request Log and assign the appropriate “Status” identifier to the “Status” section of the log (see the Helpdesk Policy).
4. After Change is Completed, the “Helpdesk” will update the “System Change Request Form” with the final status, update the Change Request Log and file all documents.

3.4.5 Related Policies

- Helpdesk Policy
- IT Asset Purchase Policy
- Digital Security Policy

3.5 IT Vendor Management Policy

3.5.1 Introduction and Goals

3.5.1.1 Policy Statement

This policy was developed to ensure effective control of contracts with all suppliers that the Local Government Unit relies on to provide them with new devices, software or services (third party). The Local Government Unit may contract a supplier to install software, remove or move computers, communications services, support staff and consultants. All suppliers must follow the standard process in this policy.

3.5.1.2 Scope

This Policy applies to all Local Government Unit employees responsible for negotiating or executing contracts for third party "Vendors" on its behalf.

3.5.1.3 Purpose

This policy seeks to reduce the risks associated with outsourcing, minimize errors by controlling costs, and raising service excellence in pursuit of increased value added and return on investment from developing the services. It also seeks to identify suppliers who may jeopardize the work of the Local Government Unit and to establish controls to reduce the associated risks.

3.5.1.4 Exemptions

The policy recognizes that not all vendor relationships are critical or will have a substantial financial impact to the Local Government Unit. Vendors meeting certain criteria (should be decided by the IT steering committee) will not be required to adhere to all components of this policy. In addition, requests for exemptions or exceptions to this policy can be submitted formally in writing to the Local Government Unit's Council. Exemptions or exceptions approvals are made in writing by the Council.

3.5.1.5 Responsibilities

1. The IT Official will create an IT steering committee made of designated IT personnel, Vendor Official, Owner of the service, and the procurement official.
2. The IT Official is responsible for supervising and maintaining this policy.
3. The policy must be reviewed by the IT Steering Committee on an annual basis.
4. Vendor official is responsible for implementing this policy and the technical management of the vendor including immediate reporting on any overall changes in risk to Local Government Unit.

5. Procurement/Financial department are responsible for the legal contracts signed with the vendor.
6. Procurement/ Financial department must abide with all related applicable Palestinian laws especially the Public Procurement Policies and Public Purchase law.
7. Procurement/Financial department are responsible for the administration of the vendor contract based on inputs from Vendor Manger.
8. IT department is the only section responsible for the safety of the Local Government Unit's IT systems and data.

3.5.2 Policies and Procedures

3.5.2.1 Assess Vendors

Develop a rule-based system to readily assess future vendors and set a minimum acceptable hurdle for the quality of any future **vendors** by reviewing data security and independent reviews. it's important to understand these risks, identify them, and how the IT department can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, reputational damage, and/or legal/regulatory issues.

1. Take inventory of all vendors the Local Government Unit has a relationship with.
2. Specify cybersecurity risks that vendors can expose the Local Government Unit to **(See IT Risk Assessment Policy)**.
3. Assess and segment vendors by potential risks and mitigate risks that are above the Local Government Unit's risk appetite; hence, it's important to thoroughly understand and assess the risks in regard to work and contractual relationships entered into with vendors:

a) **Strategic Risk:** Risk of failing to implement or achieve planned goals or initiatives. Inability to address the fundamentals required to execute the agreed strategy, as evidenced by deviations from the plans.
b) **Compliance Risk:** Risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of operational, and information security policies, procedures, and processes.
c) **Operational Risk:** Risks from a failed system of operational internal controls relating to relevant policies, procedures, and practices. Specifically, failures associated with processes, systems or people.
d) **Financial Risk**: Risks related to the financial condition of the vendors, such as a vendor under the threat of liquidation in the foreseeable future.
e) **Reputation Risk**: Risks of negative public perception and opinion, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information.

f) **Technology Risk:** Risks from any number of information technology and information governance and security issues, including inadequate resources (hardware, software or manpower).
g) **Country Risk:** Risks arising from the political, economic, and social landscape and other relevant events within a foreign country that can impact the services provided by vendors, ultimately affecting company operations.
h) **Environmental, Social and Governance Risk (ESG):** Risks related to climate change impacts, environmental practices and duty of care, working and safety condition, respect for human rights, and compliance with laws and regulations.

4. **Establish a role of "Vendor Official"** or owner of vendor risk management and all other third-party risk management practices. IT steering committee should assign the responsibility of a "Vendor Official" to an IT staff member. Regardless of who holds the vendor management role, IT official and procurement should be involved in reviewing and selecting vendors and the "Owner" of the outsourced function/process will be involved. They should have a say in evaluating necessary justifications and help approve or disapprove vendors accordingly

3.5.2.2 Writing Contracts

Contracts Information

Vendor Official under the supervision of IT official and Procurement, should review the contract to make sure that the following items are included:

a) Terms, renewals, required service levels and termination requirements.
b) The contract includes the list of services and highlights the quality standards that the provider should follow to guarantee customer satisfaction.
c) The contract also recalls the ways to redress gaps and problems.
d) Contracts that include exchange of sensitive data (as specified in the Information Security Policy) must require Local Government Unit confidentiality agreements to be executed by the vendor, must identify applicable policies and procedures (in particular Information Security policy, IT Backup policy, IT Risk Assessment Policy) to which the vendor is subjected.
e) Must identify security incident reporting requirements and possible sanctions or penalties for failure to deliver.

3.5.2.3 Inspection and Review

Local Government Unit shall have the ability to inspect and review vendor operations for potential risks to its operations or data. This review may include a planned and unplanned physical site

inspection, technical vulnerabilities testing, and an inspection of documentation, such as security test results, and disaster recovery plans.

3.5.2.4 Contract Maintenance

Departments that have implemented contracts shall ensure all contracts being renewed are updated with provisions supporting the requirements of this policy.

3.5.2.5 Reporting Requirements

1. Contracts must clearly identify security reporting requirements that stipulate that the vendor is responsible for maintaining the security of sensitive data, regardless of ownership and should produce regular reports focusing on four primary potential risk areas:

a) Unauthorized Systems Access
b) Compromised Data
c) Loss of Data Integrity
d) Inability to Transmit or Process Data

2. In the event of a breach of the security of the sensitive data, the vendor is responsible for immediately notifying the IT department/ Local Government Unit and work with them to recover and remedy the situation.
3. Contracts should include security reporting requirements in case there was suspected loss or compromise of sensitive data exchanged within 24 hours of the suspected loss or compromise.
4. **Exception Reporting:** Any exceptions from normal activity should be noted, reviewed, and the appropriate responses determined in the reports.
5. Vendors are required to comply with all the applicable Local Government Unit's Information security policies.

3.5.2.6 Non-Disclosure Agreements

a) All Third Parties who will have access to confidential information must sign a Local Government Unit IT department Non-Disclosure Confidentiality Agreement (NDA).
b) It is the responsibility of the IT department official to ensure that the agreement is signed prior to any work being performed or the release of any Local Government Unit's IT department confidential information.

3.5.2.7 Termination of Services

Termination may be required when a contract expires, the terms of the contract have been satisfied, in response to contract default, or due to changes in business strategy. Therefore; contracts must include the following:

1. Capabilities, cost, resources, and time frame.
2. Risks associated with data retention and destruction, IS connections.
3. Handling of any joint Intellectual Property rights developed during the course of the relationship.
4. Any possible reputational risk arising from contract disputes or performance issues.
5. Procurement and contract officials are to immediately ensure termination of all access to Local Government Unit's information systems and if applicable facilities housing these systems.

3.5.2.8 Monitoring

Ongoing monitoring of vendor spending performance and risks associated is an essential element of this Vendor Management policy. Vendors are monitored through:

1. Vendor Spend Analysis (Data Driven report).
2. Vendor performance.
3. Continuous Risk Monitoring.
4. Specify the vendor's technical resource tool

3.5.3 Related Policies

1. Information Security Policy
2. IT Risk Management policy
3. IT Backup Policy
4. Help Desk Policy
5. IT Assets Purchase Policy

3.6 Data Integration Policy

3.6.1 Introduction and Goals

3.6.1.1 Policy Statement

The primary objective of this policy is to standardize and control the data integration process in such a way that it achieves a balance between ensuring best practice controls, services efficiency, and information security. Integration templates must be developed in in order to support the implementation of this policy.

3.6.1.2 Purpose

The purpose of the policy is to better ensure interoperability between the information systems and more efficient use of data and data flows that results in more efficient business operations, while maintaining the required levels of data integrity, confidentiality, availability, and accessibility according to the digital security policy.

3.6.1.3 Scope

This Policy applies to all Local Government Unit's digital data, information systems, employees, and service providers.

3.6.1.4 Roles and responsibilities

1. **Business departments:**

a. Request data integration.
b. Approve implementation plan.
c. Test and review after implementation.
d. Requests for improvements.
e. Get approval from the related parties and then the GM for integration implementation.

2. **IT Official:**

a. Study the requested integration.
b. Analyze the integration and identify integration requirements and costs.
c. Form integration team from the related parties.
d. Plan and implement the integration after getting approval from the General Official.
e. Follow-up for providing business support and improvements.

3. The General Official:

a. Approve the proposed integration that is feasible based on IT reports and approved by the related parties.

3.6.2 Policies and Procedures

3.6.2.1 General Concepts

1. The data will be consistently interpreted across all the Local Government Unit systems according to the approved information systems policies.
2. Data administration should ensure that the needs of users of the Local Government Unit's data are taken into consideration in the development and modification of IT systems, data structures, domains, and values.
3. It is the responsibility of each data steward to ensure the correctness of the data values for the elements within their charge.
4. The ownership of data across the different systems should be identified.
5. Integrity of data should be controlled based on business requirements and based on users' needs. For example, different users may have the authority to change specific fields of data based on their business requirements and based on a preapproval from the data owner.
6. An electronic log of access and change on the data must be kept including the identification of the information system that is used to change data. It is not allowed to clear the log without preapproval from the GM and notifying the audit department.
7. Integration must consider the least privileges and least access to data, in addition to the other information security requirements.
8. Documentation (metadata) on each data element should be maintained within the premises of the Local Government Unit with read access abilities from the audit department. This metadata will include both the technical representation/definition of each element, as well as a complete interpretation that explains the meaning of the element and how it is used, by whom (job role).
9. Integration requests come from the business departments, signed from the department's head. The feasibility of integration is conducted from the IT department's head after getting approval on integration from the data owner.
10. If the integration is feasible, the IT department should:
    - Analyze the integration requirements.
    - Summaries the data, and metadata.
    - Review access rights and SW requirements.
    - Check need for external support requirements.
    - Detail information security requirements.
    - Review with the related departments and obtain signed approvals.

As a final step, IT department will raise it to the GM to get final approval with budget for implementation.

11. IT department will lead the integration implementation, review, and test with the related parties before going live with the integration.

12. Systems and data integration should not breach the Local Government Unit's contracts with suppliers and service providers.
13. Systems and data integration should comply with laws and the approved policies and adopted standards.
14. Integration with external systems that requires data transfer through WANs must be fully encrypted.
15. Post integration review should be conducted by the related business departments after implementation for assessment and improvement.

3.6.2.2 Integration process

The data integration framework provides the structure through which data integration requests can be made through the IT department, and ensures that the data integration is well managed and completely documented. The data integration process consists of **four phases** that lead to successful achievement of the integration purpose, and complete documentation of an accurate and comprehensive record of the data flow which will assist in tracking the information usage within the Local Government Unit, and enable future improvement.

Phase A: Analysis of the integration Requirements:

This phase is to be completed by the IT department and the integration request owner. The purpose of this phase is to clarify and document the current situation of the data and systems so as to prepare for the migration to the new situation and inform the request owner with all the implementation needs.

The following steps should be followed:

1. **Describe the request and its purpose:** This step provides a brief documented summary of the integration request including:

a. The purpose of the integration.
b. The benefits of the integration.
c. The affected users and administrators of the application (e.g. all staff, Licensing staff, water services staff, ….).
d. Identification of the affected electronic systems with details.

2. **Describe and document the current situation (before integration):** Provide a brief written summary of existing data feeds to and from this application (if any exist). It may be useful to use data flow diagrams.
3. **Provide description of the data that is involved in proposed integrations:** Clearly describe the data that is affected by the integration and the new data \ data attributes (metadata). This information is used to help define the Local Government Unit data feeds and flows, and to identify which system (or combination of systems) is authoritative for specific data.

4. **Describe the new data flow (on high-level):** Provide a high-level description of the desired data flow by the integration request. This should include the preferred data consumption method, the frequency of data transfer, the transport methodology used. (Examples might include a flat-file nightly feed, direct database querying, LDAP querying, web service querying, etc.). Data flow diagram will be useful in this step.

Phase two (B): Determine the required Work and resources

This phase is to be completed by the IT, based on their experience and knowledge of the data infrastructure, departments' requirements, and users' responses. The purpose of this phase is to determine the amount of work, resources, and budget that are required to implement the integration, and allocate the resources appropriately.

1. **List new and existing related data:** List the use of enterprise data fields and data processing rules, both new and pre-existing, that will be integrated.
2. **Define data feeds used to implement integrations:** Provide a definition of the data feed(s) that will provide the required data to the requested integration. This guarantee the awareness of all the related parties of where data is being passed to and from, and will maintain a documented and understandable flow of data over time.

3. **Detail data transport methodologies:** Provide details of how data will be transferred to and from the application. This should include the Mechanism, the Technology (e.g. SFTP, SQL), Frequency of transfer. In addition, include the details for logging, error handling and correction, and failure alert procedures.

4. **Work estimation and scheduling:** Identify available resources, estimate the work involved with each aspect of the project, and prepare a project plan. This overview should provide a high-level description of the work to be undertaken, the people involved with this work, and the expected delivery date.

Phase three (C): Test, Deploy, Monitor

This phase is to be completed by the IT and the integration requester. After completion of security assessment, a test should be conducted and evaluated for suitability of integration.

1. **Security Assessment:** Conduct a security assessment of the proposed application platform and transport methodology. Ensure that the security responsibilities of the related parties are clear and understood. Commitments to suitable security precautions and procedures should be received in writing and logged.

2. **Test:** Set up test of data feeds and test application integration. This step should ascertain the fitness for purpose of the feeds, and whether they enable the application to perform as desired.
3. **Deploy data feed:** Set up, configure and document the system and processing to provide the required data feed as a robust production service.
4. **Monitoring and logging:** Set up a monitoring system to automatically monitor the data integration process. This will enable detecting any failure.

Phase four (D): Service Responsibilities, Boundaries, Documentation

1. **This section is to be completed by the IT and the integration requester**. It sets up the ongoing policies and procedures, which will govern the use of the data feeds and integration.
2. **Legal compliance, Data protection:** Outline the data protection responsibilities and procedures associated with the application. Provide contact details of those responsible for data. Detail any further legal or policy compliance issues.
3. **Define support structure:** Clearly define the division of responsibilities for Application User support and IT helpdesk support, documenting contact details for each.
4. I**dentify any Shortfalls:** Provide information about any identified or possible shortfalls in the integration solution that is provided by IT.
5. **Documentation:** The IT must update their own documentation to reflect any changes made; the integration requester and the related parties must also review and update their own documentation.

3.6.2.3 Compliance with related policies and standards

1. The integration process should comply with the applied laws in Palestine.
2. The integration should be compliant with all IT policies.
3. The integration should be compliant with the digital security policy and all security procedure applied in the Local Government Unit and on the national level.

3.6.3 Related Policies

1. Risk Assessment policy.
2. Password Change Policy
3. Disaster Recovery Policy

3.7 Password Change Policy

3.7.1 Introduction and Goals

3.7.1.1 Policy Statement

This policy is established to regulate access to any of the Local Government Unit's systems with a login information made of username and a password. The goal is to protect the overall security of the Local Government Unit, in particular the confidential, restricted information and data from all possible threats. The policy establishes:

1. Reasonable assurances that the use of Local Government Unit systems is limited to authorized individuals.
2. Reasonable assurances that access to any Local Government Unit program source code is limited to properly authorized individuals.
3. Reasonable assurances that sensitive systems identified are isolated appropriately.
4. Guidance on the responsibility of the End user for password management and protection.

3.7.1.2 Purpose

The purpose of the policy is to protect the confidentiality, safety, integrity and availability of all restricted information created, received, transmitted and stored by the Local Government Unit's electronic systems.

3.7.1.3 Scope

This policy applies to all users of information assets including employees, (full time and part time), vendors, business partners, and contractor personnel and functional units regardless of geographic location. This Policy also covers all Information Systems environments operated by or contracted with a third party including:

1. All Local Government Unit's staff members using the Local Government Unit electronic mail facilities, email systems or messaging functions to store or transmit information including general, confidential and restricted information.
2. All Local Government Unit's electronic communication facilities.
3. All messaging functions including instant messaging.

3.7.1.4 Responsibility

This policy applies to all Local Government Unit employees who are responsible to ensure that the use of its electronic communication facilities comply with the guidelines set out in this policy.

3.7.2 Policies and Procedures

3.7.2.1 Password Management

Access and usage of the Local Government Unit's Network Domain and electronic systems must be controlled using procedures that comply with the following password management requirements:

a. Must use a Strong Password using the following instructions:

1. All passwords should be treated as confidential information.
2. Passwords should be at least 8 characters long.
3. Passwords must use a combination of upper- and lower-case letters, with random combination of numbers and punctuation marks interspersed throughout as much as possible. It is insufficient to simply use a number at the beginning or the end of the password.
4. No repeated numeric or alphas are permitted such as (333 or AAA); or a string of numbers or letters like "1234" or "abcd".
5. Names or words must not be used (found in a dictionary).
6. Password that would be hard to guess must be chosen.
7. User name must not be used in the password.
8. User Passwords must be changed every ninety (90) days automatically from the last update.
9. Administrator passwords must be reset every thirty (30) days and local admin passwords will be reset every 180 days. All service account passwords must be reset once a year during maintenance.
10. Newly created passwords must be different from the previous Ten (10) passwords used.
11. Intruder detection should be enabled to prevent further login attempts after 3 failed attempts. The timeout period before the login counter is reset should be fifteen (15) minutes and enforce and the account should be locked for at least minimum of thirty (30) minutes and a maximum of three (3) hours;
12. Do not allow the system to provide Password Hints;
13. Disabled accounts for more than sixty (60) days will be deleted.
14. Establish protocols to identify and verify the users before surrendering new, initial, temporary or replacement passwords. New accounts should receive only an initial password to be used for the first log in the system and it is allowable to surrender it verbally to the user.
15. All initial passwords must be changed when it is officially launched and used for the first time, and a three (3) day expiry period must be imposed to compel the user to change it.

16. Use multi-factor authentication to reset passwords (if it is possible) such as sending a verifying text message to a mobile number associated with the account.
17. Administrator must change immediately the passwords in case there was a suspicion that it has been compromised or as a precaution measure when released to technicians performing maintenance and support.
18. Users must acknowledge receiving the initial passwords and they should sign on the “Local Government Unit” confidentiality clause to secure passwords. This could be included as part of the Employee job conditions.
19. There should be a list of banned ‘trivial’ passwords, enforced automatically.
20. Whenever possible, the password change requirement will be enforced by technical means.

3.7.2.2 Passwords for Remote Access Users

Access to the Local Government Unit’s networks via remote access must be controlled using either a one-time password authentication or a public/private key system with a strong passphrase which is what this policy recommends. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access. All of the rules above that apply to passwords apply to passphrases.

3.7.2.3 Passwords are Authority to Act

Each computer system user is given a user ID and password that allows them to perform their authorized functions. Local Government Unit considers any action taken under a user ID and password as the sole action of the person to whom the user ID and password were assigned, and that the person shall bear full responsibility for the action. Hence; passwords are issued on an individual basis and must not be shared. For the protection of the Local Government Unit, IT department information and the employee, sharing user IDs and passwords are prohibited.

Special cases

a. If a critical business need exists and there is no other alternative to sharing a user ID and password, an Information Security Exemption Request Form (Appendix 7) should be submitted to the Information Security Officer for approval.
b. Passwords are the property of the Local Government Unit and must be surrendered by an employee when requested by their official. Failure to do so can be grounds for immediate termination.

3.7.2.4 Passwords Storage

All system passwords including but not limited to, service passwords, master passwords, application passwords, database passwords, administrator passwords, domain admin passwords

must be documented (electronically and physically) and kept in a protected safe that can be accessed only by the Local Government Unit's General Manager. It's advisable but not required to maintain the password list in an off-site location outside the main office. System passwords must be changed maximum every six months.

3.7.2.5 Reporting Compromises of Passwords

When any employee has a reason to suspect that their password has become known to another person, the password should be changed and the Information Security Officer should be notified immediately via the Help Desk. Passwords must be immediately changed if they are suspected of being compromised, or have been disclosed to anyone besides the authorized user.

3.7.2.6 Granting Access and Privileges

1. No individual will be granted a user ID or otherwise be given privileges to use Local Government Unit's IT department information systems unless advance written approval has first been obtained from the appropriate official or the Human Resources department confirming his/her status as an employee and which access rights are needed.
2. Access privileges must also be appropriate to an employee's job responsibilities.
3. Access privileges granted to users who are not an employee of the Local Government Unit will only be granted for the period needed to do the task.
4. Users who are not Local Government Unit's employees must have their privileges reauthorized by the appropriate department official.
5. Non-employee user accounts must be configured to automatically expire at the estimated end of the engagement.

3.7.2.7 Revoking or Changing Access and Privileges

1. All physical and logical access to Local Government Unit's facilities and systems must be disabled immediately upon the employee termination from the Local Government Unit.
2. Immediate changes to all master passwords to the vital systems should be imposed in case a senior member of the IT department has left the job.
3. Department officials must promptly report all significant changes in employee duties or employment status to the Human Resources Department and Help Desk, including changes for Third parties.
4. Once approved or validated, the Help Desk and/or Human Resources must notify all of the appropriate system and application administrator(s) responsible for making such changes. Once notified of terminations, system and application administrators will disable and/or remove all user access from all appropriate systems and recover all information systems equipment belonging to the Local Government Unit.

5. Only employees are authorized to be notified of terminations. Non-employees should not be included on termination notifications. Access should be removed based on the user's last day on Local Government Unit premises, which could occur before the last day of employment.
6. For personnel transferring to a different position, officials and/or the Human Resources Department must immediately submit requests to the Help Desk to ensure that all of the appropriate system and application administrators remove access to various information systems where appropriate.
7. Requests for privilege changes must also be in writing and approved by the user's official before a Systems Administrator fulfills these requests.
8. Any disputes concerning access privileges will be referred to the Information Security Officer for resolution.
9. Systems Administrators must promptly revoke all privileges no longer needed by users.
10. At least every twelve months, management must reevaluate the system and/or application privileges granted to users.
11. Depending on the criticality of the application or system, more frequent reviews may be needed.

3.7.2.8 Terminal and Workstation Controls

Per the Information Security policy, all users must secure their computer workstation whenever leaving their immediate work area. Screen savers must be invoked with the password protection feature if the keyboard or mouse is not used for a period of time. At the end of each workday, users must logoff all applications and systems.

3.7.3 Related Policies

1. Helpdesk Policy
2. Data Recovery Policy
3. Risk Assessment Policy
4. Information Security Password

3.8 IT Outsourcing Policy

3.8.1 Introduction and Goals

3.8.1.1 Policy Statement

This policy applies to the "Outsourcing" or "using external sources "or "Third Parties" of a Local Government Unit owned activity and entering into agreement with third party "Vendor" to perform the activity on continuing basis. Outsourcing enables the Local Government Unit to take advantages of external entities that can provide services for a fee with the goal to manage costs and access capabilities that are not available in-house.

The policy covers the following:

- Third-party risk assessment.
- Agreements and contracts.
- Providing network services.
- Access rights for systems and networks.
- Third-party access security

3.8.1.2 Scope

This Policy applies to all Local Government Unit employees responsible for giving vendors or "Third Parties" access to the Local Government Unit's network or its connected systems who are engaged in delivering services on its behalf (whether Individuals, companies, institutions, contractors, consultants or specialists)

3.8.1.3 Purpose

This policy provides directions in assessing whether and how an IT service or related activity can be appropriately outsourced. Outsourcing arrangements should neither diminish the Local Government Unit's abilities to fulfill its obligations to citizens, nor impede effective supervision by its designated employees.

3.8.1.4 Responsibilities & Roles

1. The official in the department that has the "Outsourced function" is considered the "Owner" of the outsourced function/process.
2. Vendor Official will manage the relationship with the Vendor and will follow up on the implementation of the outsourced services.

3. A committee made of the Vendor Official, IT official, procurement official and "Owner" are authorized to select providers or "Vendors" for outsourcing of the Local Government Unit function/process.
4. IT official will overlook the implementation of this policy.

3.8.2 Policies and Procedures

3.8.2.1 Outsourcing Principals

1. Identification and Documentation: creating a formal strategy and vision;
2. Outsourced Services should be subject to the same management disciplines that would apply as if the service was not outsourced.
3. IT department has to ensure that Outsourced Services will be clearly shown on the organizational chart of the Local Government Unit.
4. Each outsourced service may have a position description created for it in the same way as if the service was being performed internally. The position description is filed with other documentation pertaining to the service provider.
5. Outsourced Services should ideally be the subject of documented agreements that include service level agreements, review processes, period of service, details of service, limitations on outsourcer activities, risk management requirements, financial and capacity issues, termination, insurance and dispute processes
6. Technically, the Law on Confidentiality and Security of Information concerning Local Government Units must be applied.

3.8.2.2 Due Diligence

Appropriate due diligence as outlined below must be used when considering the outsourcing of an activity and selecting third party "Vendors", with capabilities to implement especially that risk management and compliance are transferred to Third Parties who might fail in delivering the required services; hence, the Local Government Unit will be held responsible. A rigorous Risk Assessment process must be followed to assess providers of outsourced services against the following criteria:

3.8.2.3 Outsourcing Selection Criteria "Third Party"

Criteria for selecting a provider for Outsourced Services shall be defined and documented, taking into account the:

1. Length of Experience - the company's reputation and history;
2. Quality of services provided to other customers: evidence of any previous work and

demonstrated level of expertise
3. Number and competence of staff and officials;
4. Financial stability of the company;
5. Dispute resolution performance;
6. Disaster recovery performance;
7. Responsiveness and Communications standards;
8. Ability to deliver on time;
9. Possible conflicts of interest;
10. Quality assurance and security management standards currently followed by the company (e.g. certified compliance with ISO 9000 and ISO/IEC 27001);
11. Further security criteria defined as the result of the risk assessment) see **IT Vendor Policy)**

3.8.2.4 Strategy and Risk Assessment

1. The Vendor official and the "Owner" should be identified.
2. The owner shall assess the risk before outsourcing the service.
3. The owner shall consider the impact of the outsourced service.
4. The Vendor Official and the "Owner" shall review the assessed risks before the function/process is outsourced, using the selection process outlined above.
5. The Vendor Official and the "Owner" will review the impact on existing systems, the nature of logical and physical access to the Local Government Unit's information assets and facilities required by the outsourcer to fulfill the contract **(see Information Security Policy and Vendor Management Policy)**;

a) **Establishing Connection: Any** connection with the Local Government Unit systems should be based on the least authority principal according to the needs of the work and the revisions.
b) **Change or alterations of access:** Changes in access should be made according to the needs of the job and should be reviewed for security. Change Management should be used to deliver the changes.
c) **Third Party permitted access:** Third parties and any other Local Government Unit partners are permitted to access the its systems according to what has been agreed on in the signed contracts. Access could be physical and online.
g) **Third Parties are allowed** to access the data and services that will enable them to do only their jobs according to the signed contracts and the request submitted.
h) Sensitivity, volume and value of any information assets involved.
i) Commercial risks such as the possibility of the outsourcer's business failing completely, or failing to meet agreed service levels.

j) All proposals for outsourcing contracts regardless of total costs must be presented to the Council of the Local Government Unit for approval prior to entering into any commitments/contracts with the vendor.
k) The Council will study the contract to ensure it is aligned to organizational strategic goals and shall decide if the Local Government Unit will benefit from outsourcing the function, taking into account the information security aspects. If the risks involved are high and the Local Government Unit's benefits are marginal (e.g. if the controls necessary to manage the risks are too costly), the function shall not be outsourced.
l) Related risk information should be recorded as stipulated in the **Risk Assessment Policy**.
m) If a Third Party has access to "sensitive data", a periodic review should be done to obtain reasonable assurance on the controls and operational effectiveness of the outsourced service provider and must demonstrate compliance with the Local Government Unit's IT Security Policy.

3.8.2.5 Confidentiality & Written Contracts

Outsourcing relationships should be governed by written contracts that clearly describe all material aspects of the outsourcing arrangement, including the rights, responsibilities and expectations of all parties.

1. A formal contract between the Local Government Unit and the outsourcer shall clearly define the parties to the contract, effective date, functions or services being provided (e.g. service levels), liabilities, limitations on use of sub-contractors and other commercial/legal matters normal to any contract.
2. The contract shall clearly define the types of information exchanged and the purpose for this doing. If the information being exchanged is sensitive (Confidential), a binding confidentiality agreement shall be in place between the Local Government Unit and the outsourcer, whether as part of the outsource contract itself or a separate non-disclosure agreement;
3. Third Party must enter into binding service level agreements that specify the performance to be delivered and the remedies available in case of non-compliance.
4. Local Government Unit must take steps to ensure that service providers protect confidential information from intentional or inadvertent disclosure to unauthorized persons. This is addressed in the **IT Information Security Policy** and **IT Vendor Management Policy** and Procedures.
5. Depending on the results of the risk assessment, various additional controls must be embedded or referenced within the contract to monitor all access to and use of the Local Government Unit facilities, networks, systems etc., and to allow the audit of the outsourcer's compliance with the contract.

6. Following review by Procurement Services and ensuring that the Local Government Unit privileges are clearly stated, all contracts shall be submitted to Municipalities Legal Consular for final approval.

3.8.2.6 Managing Disputes

It is expected in any Outsourcing relationship to have occasional conflicts of interest and possible breaches which arise as a result of devirginize from mutual interests. It stands as a risk that has to be considered by the Local Government Unit. Whether actual or potential, Local Government Unit must a adopt a model to resolve anticipated concepts based on the suggested following Processes:

Where a dispute or a breach of contract arises with **Outsourcers**, the "Vendor Official" and "Owner" would immediately end the conflict through the following

a) **Control Conflicts**:

1. Identify the conflict (present or future).
2. Assess the seriousness of the conflict and evaluate effects.
3. Decide on a response and how to implement it.
4. Ensure services are not significantly affected.

b) Disclosing Conflicts:

1. Outsourcers have to engage with the "Vendor Official" and report any conflict of interest that may arise in relation to the provision of services.

c) Avoiding Conflicts:

1. If a conflict of interest would have a major impact on the Local Government Unit, it must be avoided at any cost until the control or disclosure processes are enough to solve the issue.
2. In this case, the "Vendor Official" would ask IT official to intervene to avoid the conflict.
3. IT official must resolve the conflict within 14 days and depending on the seriousness of the matter, the following alternative measures can be adopted if the conflict is not rectified:

I. Accept the failure / breach of the supplier.
II. Refer the matter to relevant alternative dispute resolution facilitators.
III. Refer the matter to Local Government Unit legal advisers.
IV. Recommend termination of the supply contract or agreement to the Local Government Unit's Council for their consideration.
V. Recommend to the Local Government Unit's Council a replacement services from an alternative supplier.

3.8.2.7 Monitor and Evaluate

(Please check also Vendor Management policy for more information)

1. Vendor Official (First line of Defense) shall provide performance reports including risk, compliance and assessment reports on monthly basis;
2. IT official (2nd line of Defense) will report to Local Government Unit's Council on the outsourcing arrangements annually;
3. The Local Government Unit's internal audit department (3rd line of Defense) must review any proposed outsourcing of a functional/process activity and regularly review and report to the Council on compliance with the Local Government Unit outsourcing policy.
4. Local Government Unit's Council to evaluate outsourcing services and officially approve/change Outsourcing activities.

3.8.2.8 Intellectual Property

The Local Government Unit is the sole owner of all documentations, files, databases, software, graphics or any other content generated or designed or developed or purchased by the "vendor" for the Local Government Unit and is considered its property and shall remain as such following the termination of the agreement with the vendor.

3.8.3 Contingency Plans

IT Department should follow the Disaster Recover Policy and Backup policy to establish and maintain contingency plans.

3.8.4 Related Policies

1. Digital Security Policy.
2. IT Risk Management policy.
3. IT Vendor Management Policy.

3.9 Information Security Policy

3.9.1 Introduction and Goals

3.9.1.1 Introduction

Security measures should be appropriately tailored to the social and citizen-oriented services of the Local Government Unit, and most importantly the Council should view the security measures as a strategic asset, part of a profit center, rather than only as a cost center. In this policy, we strongly advise not to look at the security level as one-size fits all model since municipalities differ in capacities and management abilities. However; regardless of the size of the Local Government Unit, digital security should be approached holistically as a single policy area as stipulated in this systematic digital security approach. **Change Management Policy, Helpdesk Policy, IT Purchase Policy, Password Policy, Backup Policy, Risk Assessment Policy** contemplates the Policy.

3.9.1.2 Policy Statement

Computer system resources and associated data are business critical municipal assets. Sufficient measures should be taken to ensure that all the Local Government Unit's policies, standards, procedures and guidelines have been established to address administrative, technical, and physical safeguards to:

1. Ensure the security and confidentiality of Citizens/Customer records and information;
2. Protect against any anticipated threats or hazards to the security or integrity of such records;
3. Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

3.9.1.3 Scope

This policy applies to all Local Government Unit's employees, service providers, vendors and agents using its computers or personally-owned computer or workstation used to connect to the its network, as well as to remote access connections used to do work on behalf of the Local Government Unit, including reading or sending e-mail and viewing intranet web resources; therefore, the following are covered by this policy**:**

1. Full-time and part time employees of the Local Government Unit,
2. Volunteers who are authorized to use the Local Government Unit 's resources to access the Internet.
3. Local Government Unit contractors who are authorized to use their equipment and facilities.

3.9.1.4 Purpose

The purpose of the policy is to better ensure the confidentiality, safety, integrity and availability of all digital information created, received, transmitted and stored by the Local Government Unit's electronic communication facilities. This objective will be achieved by integrating **digital security** governance within the overall risk management practices of Local Government Unit as stipulated in the **Risk Assessment policy and Backup Policy**.

3.9.1.5 Responsibilities

The following guidelines intend to assist users maximize the benefits attained from using IT department resources at their disposal according to the following measures:

1. IT Official to designate specific personnel as "Security" officer to handle Local Government Unit 's security incidents and issues.
2. Users are individually responsible for protecting the data and information they work with.
3. Where users are uncertain about the sensitivity of information, the head of department must be approached for assistance.
4. Users must immediately report anything unusual about data or information on their computers to their head of department.
5. People who appear to be strangers in a work area may be confronted by employees to determine the purpose for their presence.
6. Equipment must be protected from theft and kept away from food and drinks.
7. It is preferable that data must be stored on a network drive (not local c: drive) to ensure that data is backed up regularly as stipulated by the **Backup Policy.** In case, the Local Government Unit chooses an outside "Cloud" Solution, the **Vendor Management Policy** and **IT Outsourcing Services Policy** applies.
8. Officials must immediately inform IT to revoke access rights when an employee or a Third Party has ended their work; or does not need access privileges anymore or any for any other reason they may see fit.

3.9.1.6 Ownership of Information

All information generated by employees or consultants on any Local Government Unit project is considered its property, therefore; must be protected by the Local Government Unit according to its classification.

3.9.2 Policy and Procedures

3.9.2.1 Policy and standard Requirements

To avoid accidental loss scenarios and mitigate declared risks (according to the Risk Assessment Policy), the Local Government Unit needs to increase the user awareness (regardless of their position). The basic components of this digital security policy are based on:

Data Classification: Not all information requires the same level of protection. The level of protection applied to data must be appropriate with its classification to ensure appropriate handling and disclosure. The classifications are either Public, internal use only or Confidential:

a) Public Classification

Information available to the public and is likely to be found on the Internet. Examples of Public information are press releases. Public information does not require any special handling or markings.

b) Internal Classification

Information, due to its business sensitivity or technical content, is intended to be distributed only internally. Examples of internal information are employee handbooks, telephone directories, routine administrative of office information, organizational charts, and policy and standards. All "Internal" information that is shared with others must be marked "Local Government Unit Internal Use Only." All information is considered "Internal Use Only" by default. Information, which has not been classified, is to be treated as "Internal Use Only".

c) Confidential Classification

Information whose unauthorized disclosure, compromise, or destruction could have an adverse impact on Local Government Unit's reputation, customers, or employees, or expose it to financial loss must be classified as "Confidential". Examples of confidential information are Citizen's account numbers or Citizens lists and requirements, computer data, and employee information or the Local Government Unit plans, budgets, personnel records, system configurations, network addresses. The failure to designate particular information as confidential and/or proprietary shall not preclude any later claim by the Local Government Unit that such information is confidential and proprietary. This includes information generated outside the Local Government Unit's premises if the information is part of its activities. Confidential information must be protected and backed up as stipulated in the **Backup Policy** and therefore requires special handling and labeling as described below.

3.9.3 Grant Least Privilege – according to knowledge needs

Access to data must be determined on the basis of the need for knowledge, taking into consideration the classification of the data and the risks identified (**with reference to the Risk Assessment policy)**, and therefore a staff member must be granted access to IT systems based on the minimum number of privileges required to perform the function and unless there are risks associated with access, this policy outlines the requirements for data accidental leakage prevention by employees using various security controls including or users by reviewing the following security controls:

1. Discretionary Access Control (DAC)

This policy recommends (DAC); one of the dominant forms of authorization; which manages access using ACL (Access Control Lists) on each resource object where users are listed along with the permissions or privileges granted or denied to them.

a) System owners will establish appropriate access control standards for their information systems and will authorize access to them.
b) **Access control list** should only include authorized Local Government Unit employees, IT department employees who perform database maintenance and administration or a designated approved contracted 3rd party including the appropriate access rights or privileges granted.
c) Only Authorized individuals should have access to the supported databases at the Local Government Unit. Please note that the Helpdesk policy established procedures to handle immediate changes in the rights to access the systems whether employees or Third parties.
d) By default, most restrictive access should be applied to the database and allow access only based on need-to-know basis.
e) Database access list should be reviewed at regular intervals to insure only authorized users are able to connect to the database or perform local tasks.

2. Impose controlling access through:

a) Physical Security: A security measure to secure the physical location of the IT equipment:

1. The IT department, as part of its **asset management**, must conduct a physical inventory of computing equipment on an annual basis, accounting for the location of the assets.
2. All computing equipment should have serial numbers and property tags recorded in the Local Government Unit's asset system for identification purposes, should this equipment become damaged or stolen as stipulated in the **IT Purchase Policy**.

3. Employees are expected to be aware of equipment located within their immediate offices and to immediately report missing equipment to supervisors.
4. Employees suspecting any form of security breach must report it to the department official. This includes but not limited to unauthorized entry, doors left open, locks not working, doors left unlocked or not closing properly, security codes divulged to unauthorized personnel and lost secure IT room keys.
5. Anyone noticing suspect or unknown personnel in an IT room must immediately either challenge the individual directly, or report the incident to the official;
6. Automated protection (protected screen password and keyboard lock) should be activated on servers, computer stations, workstations or small computers if there is no activity for a predetermined period of time to prevent illegal system access,
7. Human Resources department must inform the IT Department official about any changes in the contracts of any employee such as dismissal or end of contract or change of position which entails changes to permissions to reach the network and or cancellation of accounts and usernames.
8. Any instances leading to security breaches resulting from staff not following the above guidelines may be considered a disciplinary issue.

b) Internal Access

1. The Local Government Unit shall utilize access control systems for all locations processing and containing critical data or hosting technology assets/equipment.
2. IT should create a list of IT rooms and authorized staff and should be kept in a register, including staff and contractors granted temporary permits.
3. Line Officials must inform employees with access to locations processing and containing critical data or technology assets/equipment about potential risks and measures used to control them.

c) External Access

Any access between an external party and the Local Government Unit must be approved by the IT department. **Secure remote access** must be strictly controlled with the following requirements:

1. Remote access to the Local Government Unit's network will be absolutely prohibited using User registration process.
2. IT owner will approve requests to access the systems. The note will include: name of person, Employee or "Third Party", Contract period, reasons for requesting the access;

3. Remote access will be allowed only on **Need** basis and for work related tasks to a limited period. If more time is needed, another note must be submitted stating the reasons for the new request.
4. Control will be enforced via one-time password authentication. For information on creating a strong pass-phrase see the **Password Policy**.
5. All remote access to be controlled through limited number of Municipal access points and must be point-to-point encrypted.
6. All remote access connections must be registered including the Internet protocol address and the User name.
7. Employees and service providers with remote access privileges must ensure that their Local Government Unit owned or personal computer or workstation, which is remotely connected to the Local Government Unit's corporate network, is not connected to any other network at the same time.
8. All end users should be made aware of the supporting security standards and related procedures.

3.9.3.1 Change Management

1. **Change Management policy** protocols should be applied in the case of any changes to the Local Government Unit's systems; in particular the "Software Patch" updates.
2. It must be tested prior to implementation and must be implemented by the designated party (the developer or the seller) who has a contract with the Local Government Unit.
3. In case a remote access is needed, the access control measures apply.

3.9.3.2 Separation-of-Duties

No single individual should control an entire critical/ operational IT process. Checks and balances must be implemented to reduce the chance of fraudulent activity. IT Department must identify the relevant IT roles for their Information Systems. Once identified, Separation of Duties must be implemented such that critical/operational IT functions are separated into distinct jobs to prevent a single person from harming a development or operational system or the services it provides, whether by an accidental act, omission, or intentional act. The roles identified (and implementation of Separation of Duties) must be listed in the particular Information System's security plan.

3.9.3.3 Security Auditing

1) IT systems hosted and maintained by the Local Government Unit will be periodically tested for known vulnerabilities and security flaws;
2) Applications hosted and maintained by third party providers, such as cloud Software as a Service (SaaS) systems, must be tested at least once annually.
3) Vendors must provide a proof of testing prior to upload the Local Government Unit's data or entered into the application.

3.9.3.4 Secure Disposal of Information

When "Confidential" paper documents are to be destroyed, destruction must occur either by shredding the document or placing it in a locked shred bin. All Local Government Unit's service centers that receive written forms should be equipped with this type of machinery.

3.9.3.5 Security of Removable Media

All data backup tapes must be stored in a secure location and this environment must be

conducive to storage of magnetic media and operational use of computer equipment as stipulated by the **Backup Policy**. If this is not possible then backup media must be allowed time to re-adapt to operational conditions before use.

3.9.3.6 Off-site storage

Per the "**Backup Policy**", all backup media taken off-site should be logged in and out to ensure that all copies of data can be located if required, and off-site depositories can be audited.

3.9.3.7 Media in transit

Computer media can be vulnerable to unauthorized access, misuse or corruption during

transportation. The following controls should be applied to media in transit between sites:

1. Media should be encrypted and the key should be kept in a safe location under the direct supervision of the General Manager of the Local Government Unit.
2. Reliable transport or couriers should be used.
3. Packaging should be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with manufacturers' specifications.
4. Media should be held in secure containers and tamper proof packaging that reveals any attempt to gain access.

3.9.4 Information on Personal and Shared Directories

An employee can only store "Confidential" information either on his personal directory or another designated directory located on a Local Government Unit's server in a secure server room. No Confidential information will be stored on a local drive of a desktop computer. For laptops, "Confidential" information stored on the local drive must be encrypted using Local Government Unit's IT department configured and managed software. Unless absolutely necessary and approved by the Management of the Local Government Unit, "Confidential" data should not be stored on a laptop.

3.9.5 Backup Plan

The IT department should create a **Backup Plan** as part of any emergency plans to protect the Local Government Unit's data. It adheres to an action list created prior to software or system integration and it includes detailed steps and techniques for uninstalling or de-integrating a new system, as well reversing process changes. Please check also the **Integration Policy and Change Management policy** for more information.

3.9.6 Password security

As stipulated in the **Password Policy**, Passwords are an important aspect of computer security and the front line of protection for user accounts. A poorly chosen password may compromise the Local Government Unit's entire corporate network. As such, all employees (including service providers and vendors with access to the Local Government Unit's systems) are responsible for taking the appropriate steps, following the NIST guidelines instructions; to select and secure the passwords:

a) Enforce a strong Password:

1. All passwords should be treated as confidential information
2. Password that would be hard to guess must be chosen;
3. Each password must be at least eight (8) characters in length,
4. User name must not be used in the password;
5. No repeated numeric or alphas are permitted such as (333 or AAA); or a string of numbers or letters like "1234" or "abcd";
6. Passwords must be alphanumeric i.e. must include both letters and numbers;
7. Passwords must use a combination of upper- and lower-case letters, with numbers and punctuation marks interspersed throughout as much as possible. It is insufficient to simply use a number at the beginning or the end of the password.
8. Names or words must not be used: strong passwords are a random combination of numbers, letters and punctuation marks.
9. User Passwords must be changed every ninety (90) days automatically from the last update. Administrator passwords must be reset every thirty (30) days, and Local admin passwords will be reset every 180 days.
10. All service account passwords must be reset once a year during maintenance;
11. Disabled accounts for more than sixty (60) days will be deleted;
12. Password History: Newly created passwords must be different from the previous Ten (10) passwords used.

13. All initial passwords for any Local Government Unit's information system must be changed when it is officially first used and an expiration date (3 days) on its validity must be imposed to force the user to change it,
14. All initial passwords must be delivered to users in a secure manner;
15. Initial passwords must not be delivered to the user in clear text or in any easily reversible form and must not receive passwords in clear text over the network
16. Protocols must be established to identify the users before surrendering new, initial or replacement password;
17. Users must acknowledge receiving the initial passwords;
18. Establish procedures to verify the identity of the user before submitting a new, alternative or temporary password;
19. Passwords must be changed immediately if the employee suspects it has been compromised or if it was given to a technician who performed a maintenance or provided support;
20. Use multi-factor authentication to reset passwords (if it is possible) such as sending a verifying text message to a mobile number associated with the account.
21. Limit the number of wrong attempts to enter the Password to only three (3) within a period of fifteen (15) minutes and enforce a ban to entry for a minimum of thirty (30) minutes and a maximum of three (3) hours;
22. Do not allow the system to provide Password Hints;
23. Use multi-factor authentication (MFA) whenever possible to mitigate the security risks of stolen and mishandled passwords.
24. When employees leave the organization, change the passwords for their accounts.

b) Stored Passwords

1. Use a strong hashing scheme to protect user's passwords before you store them.
2. Enterprise applications must protect stored and transferred passwords for the systems (Root/Administrator) with encryption to ensure hackers won't crack them.
3. Users (and applications) must not store passwords in clear text or in any easily reversible form and must not transmit passwords in clear text over the network.

The following actions are prohibited :

1. Revelation of a password over the phone to any person.
2. Revelation of a password in an e-mail message.
3. Talking about a password in front of others.
4. Any hint at the format of a password (e.g., "my family name").
5. Revelation of a password on questionnaires or security forms.
6. Sharing a password with family members.
7. Revelation of a password to co-workers while on vacation.

c) All users must sign an article to maintain the secrecy of personal passwords. The article could be included in the hiring conditions.

3.9.7 Firewall

IT department is advised to use a Firewall to protect the IT systems of the Local Government Unit from unauthorized access and it should keep the licenses valid all the time.

3.9.8 Anti-virus measures

1. All Local Government Unit servers, desktops, and laptops must have an antivirus application installed to scan computers and media for malicious software.
2. Anti-virus programs should be active at all times when a computer is utilizing any Local Government Unit network resources.
3. The application must be configured for daily updates.
4. All electronic mail must be scanned for malicious attachments.
5. All files on electronic media of uncertain origin or files received over un-trusted networks must be scanned for viruses before use.
6. All drives must be scanned for viruses and any type of malicious code, at least once a week.
7. The Anti-virus software should be capable of monitoring systems, alerting Local Government Unit's IT department personnel and take corrective action in the event of virus detection.

3.9.9 Related Policies

1. Disaster Recover Policy
2. Risk Assessment Policy
3. Backup Policy
4. Password Policy

3.10 Help Desk Policy

3.10.1 Introduction and Goals

3.10.1.1 Introduction

The "Help Desk" or the "technical support department" is a combination of software application, business processes and support operation combined into an IT department's unit. The helpdesk is a comprehensive system through which, IT support personals utilize to provide initial resolution, manage and monitor IT support or service, requests generated from residents/ users and ensure an affective logging and tracking of issues.

3.10.1.2 Policy Statement

The helpdesk plays an important part in the IT service lifecycle. It's a single point of contact for end-users to fulfill or resolve all computer, network and business systems' related needs. The Helpdesk focuses on managing the lifecycle process of IT services which includes:

1. Helpdesk management
2. Service & Support request management
3. Technical support
4. Service level agreements' (SLA) management
5. Incident reporting
6. Change control management
7. Knowledgebase portal
8. Employees

3.10.1.3 Scope

This policy applies to all of the IT services.

3.10.1.4 Purpose

This policy establishes procedures to structure governance of all IT systems and infrastructure support activities together with the acquisition of any IT hardware, software or externally sourced IT Services; in particular:

1. To streamline and improve IT support's lifecycle processes.
2. To improve response time to service requests and reduction of time spent keeping track of requests.
3. To provide effective support to the Local Government Unit employees.

4. To provide effective resolutions to daily IT related incidents.
5. To improve staff mobilization should an incident occur.
6. To improve internal communications between IT and other unit departments.
7. To increase corporate productivity through transparent support process.
8. To leverage the helpdesk system as an oversight tool and provide management with performance metrics utilizing built in or custom reports.

3.10.1.5 Responsibilities and Roles

1. The Helpdesk shall be the first line of support and first contact with the End user.
2. The IT personnel is the second line for IT support services;
3. The Helpdesk shall ensure that the procedures are followed as stipulated in this policy.
4. IT department shall ensure that the necessary controls are in place to implement this procedure.
5. IT department shall resolve all requests for assistance on supported applications within the agreed SLA.
6. Technical support will follow the established procedures in documenting requests and communicating developments to Change requesters and affected departments, and following up on the Change request status.
7. Helpdesk will document the minutes of meetings of the Advisory Board on Regular and Emergency Changes.
8. Helpdesk will document status of the Change in the change register book record.
9. All employees are required to report any malfunction noticed in the systems or the services.
10. The IT Official is responsible for overseeing this policy.

3.10.2 Policies and Procedures

3.10.2.1 Help Desk objectives

1. Facilitate the rapid resolution of Client problems through a single point of contact;
2. Maintain a historical log of the support provided to each Client;
3. Identify user sites that are experiencing difficulty with a particular application;
4. Track the type of problems encountered for each application;
5. Uncover recurring problems and assist in planning a corrective course of action;
6. Generate statistics, such as the number and type of calls by application.

3.10.2.2 Helpdesk Services

The Helpdesk will receive all requests from End users and Business departments on all IT related services – current and new services. The following is a sample of possible services:

a) Incidents:

1. Create, update and delete users in the business application systems
2. Create, update and delete users in the domain
3. Create, update and delete user folder shares
4. Create, update and delete users in the Telephone Management System
5. Configure and install telephone handsets;
6. Addition and removal of machines;
7. Install, configure and update recommended or approved software;
8. Install and setup computer equipment and peripheral items;
9. Application software maintenance and support all requests for change;
10. Managing requests' logging, tracking and providing first-line technical support with the goal of cutting-down the number of issues from reaching second and third-tier level support by targeting a first call resolution.

b) General Support

1. First level technical support.
2. General Computing Advice: Technical support includes supporting users who are using personal computers (PCs), productivity applications such as Microsoft office, email applications or specific industry's application such as iMAL.
3. Network support services.
4. File backup and restore services.
5. Logging, Monitoring, tracking and updating tickets.
6. Service level management.
7. Assist Change management and facilitate change request notifications.
8. Utilization and performance reporting.
9. End-users' surveys (employees).
10. Provide end-users with service outage or IT notifications.
11. Provide updates on major incidents using the "Major incident Form".
12. Knowledgebase service.

3.10.2.3 Identify Priorities

ITIL uses three metrics for determining the order in which incidents are processed:

1. Impact - The effect on business that an incident has:

a) "High" (interruption to critical business processes)
b) "Normal" (interruption to the work of individual employees)
c) "Low" (hindrance to the work of individual employees, continuation of work possible by means of a circumventive solution)

2. Urgency - The extent to which the incident's resolution can bear delay or (available time until the resolution of the Incident) for example.

a) 1: to 0.5 hrs.
b) 2: to 2.0 hrs.
c) 3: to 6.0 hrs.

3. Priority - How quickly the service desk should address the incident, and (as a suggestion): the Priority values are defined as follows:

a) Priority 1 = low = 16hrs
b) Priority 2 = normal = 8hrs
c) Priority 3 = medium = 4hrs
d) Priority 4 = Critical = 2hrs

ITIL suggests that priority be made dependent on **Impact** and **Urgency** according to the following table:

	URGENCY 1	**URGENCY 2**
IMPACT 1	PRIORITY 1	**PRIORITY2**
IMPACT 2	**PRIORITY** 2	**PRIORITY** 3
IMPACT 3	PRIORITY 3	**PRIORITY** 4

Please note that the Expected Resolution Time should be estimated by the IT department; hence, the above time frame is merely an estimate, since resolution of the incident may require involvement of external parties who are not bound by time estimates indicated in the table.

3.10.2.4 Authorization

1. **Proper approvals and** authorized signatures of heads of the Business unit are required for every change request before submission to the helpdesk.

2. It is acceptable for a business unit outside IT to submit a "**System Change Request Form**" with only the requester official's signature.
3. The helpdesk will route the change to the appropriate IT personnel for further approvals per the **Change Management Policy**.
4. Local Government Unit's GM or his designee is responsible for approving or disapproving system change requests with a "High" impact status.

3.10.2.5 End-User Responsibilities

Local Government Unit employees are requested to provide detailed information when requesting a service using the right Helpdesk form.

3.10.2.6 Helpdesk forms

Helpdesk Forms should be developed to collect the right information so as to resolve a problem with an existing condition or technical environment. Check the appendix for a sample of suggested different possible forms:

1. **System Change Request**: Requests that cover installed hardware, software or service and the failure to perform or deemed failed such as broken keyboard, inability to print or access a network resource.
2. **Service Request:** Requests that cover end-user needs for new hardware, software or services (Appendix 4)
3. **New Proposals or Project Oriented Requests:** Users who request services that deem to be project oriented such as introducing new technology, software package or solutions.
4. **Major Incident Report:** Incident reporting is a Helpdesk added function to provide dual control and decrease incident reoccurrence.
5. **Information Security Incident Reporting**

3.10.2.7 Helpdesk Support Process

1. All service requests may be sent to the helpdesk team by: walk in, phone call, email to helpdesk@Local Government Unit.ps or sent via an interoffice memo.
2. Confirmation receipt during regular business hours will be sent to the requester within # of hours. End users will receive a response with a case tracking number.
3. **Request Capture:** All requests will be captured and verified in the helpdesk system to confirm that all fields are completed. If the form is incomplete, the request will be returned to the requester for completion.
4. **Request Ticket:** A request ticket will be opened in tracks with the requester's name, phone number and incident description and the right SLA parameter (**please see SLA in below section**) . If the nature of the incident can be resolved immediately, such as password reset, for instance, then the Helpdesk agent will attend to the incident immediately, and update the

logging system accordingly; and assign the appropriate "Status" identifier to the "Status" section of the log (see Status Log below).

5. **Problem Resolution**: IT will attempt to resolve all problems and requests for supported systems and applications. If the problem remains unresolved it will be escalated to the next level of support and if it may require involvement of external suppliers or service providers (Third line support), the requester will be informed of such arrangements and possible delays in the resolution of the incident.
6. **Incident Closure:** All incidents will be closed when resolution has been successfully implemented and request is "Closed" ; In the event that the incident is complicated and cannot be resolved within reasonable time periods, or that the resolution of the incident may be prohibitively costly, then the requester will be advised on available options.
7. **Customer Satisfaction:** Surveys will be established to ensure customer satisfaction. Before closing any call, the Helpdesk agent must confirm with the requester whether the incident has been resolved satisfactorily. Once the incident has been resolved, the logging system will be updated accordingly;
8. The helpdesk provides full support during Local Government Unit's business hours. In the event of an emergency or for any urgent problem that cannot wait until the next business day, end-users' should contact the on-call engineer or technician on duty at XXXX .

a) **Status Log**

Status	Definition
A - Approved	The required officials (i.e. requester's official, affected technology business owner/ official) approved and signed the System Change Request Form.
I - Implemented	The Implementer completed the change request. Testing/Validation of the change may still be required.
S-Successful "Closed"	The Implementer and/or requester confirmed successful completion of post implementation testing (if required) and validation of change.
U -Unsuccessful	The Implementer and/or requester determined the change, during the testing and validating, did not functionally meet the business requirements. If necessary, the Implementer will follow the back out plan.
H - Hold	The Requester and/or Implementer requested a hold on the change request. The business unit official may also request a hold due to additional information requirements or scheduling conflicts.
C - Cancelled	The change request was cancelled.

D - Denied	The change request was denied due to a specific reason (e.g. scheduling conflicts, resource issues, etc.).

b) Service Level Agreement "SLA"

Requests established through the helpdesk are logged in the system and given SLA parameters. The following is an example:

Severity / Priority	Business Impact Description	Examples	Response Time
Informational (5)	Customer request for information only	How do I change my default font? How do I add or change a printer	# Of working days
Low (4)	Minor impact; problem is one that results in a minor loss of service but does impact productivity. Employee requires information, installation, configuration, or deferred maintenance. Employee is experiencing noticeable problems but can still perform most operations.	My machine is slow to boot up. An application is slow to launch.	# Of working days
Medium (3)	Problem where production is proceeding but is degraded. Customer is experiencing usability problems. It is a time-sensitive issue important to long-term productivity, however not causing an immediate work stoppage or significant customer concern.	One PC is not working. One person cannot print. Customer needs MS-Office loaded.	# of hours
High (2)	Severe impact; multiple users or one mission critical user is affected and there is no work around available. Several Employees are experiencing noticeable problems which impact operations and/or instruction.	No one can print. The only computer with a business-critical application is down.	Immediate

Critical (1)	Fatal; impacts critical components of customer's production environment. More than one user is unable to access their machine or the network resources due to a single related problem. Initial indication shows critical components maybe down for over 30 minutes. System wide outages causing major impact to critical business operations and instruction.	Email service is down or Server is down and no one can access the email system at external level.	Immediate to >= 15 Minutes Notify Management

Response and update SLA*

Severity	**Acknowledgement**	**Response**	**Status update** If resolution is greater than # hours
Critical (1)	Immediate	>= 15 Minutes	Not Applicable
High (2)	>= 30 Minutes	2 hours	Not Applicable
Medium (3)	>= 60 Minutes	2-4 hours	Once every 8 hours
Low (4)	>= 4 hours	1 working day	Once every 16 hours
Informational (5)	>= 4 hours	1 working day	Once every 16 hours

***IT and management need to decide on the time frames for the above processes**

c) Client Procedure

The Client is expected to develop in-house expertise and internal processes for troubleshooting problems, escalation and resolution. Prior to contacting the Help desk, the in-house expert should make every attempt to resolve the problem by referring to the system documentation or established site- specific procedures. In-house expertise and troubleshooting procedures are important so that:

1. Problems which are procedural and unique to the Client can be solved by the appropriate Client authority;
2. Minor problems can be resolved without any delay;

3. Issues related to staff requiring additional training identified and timely corrective actions can be taken.

d) End User Escalation

End User or Helpdesk agent may initiate "Escalation" if they feel a request is not being handled on timely basis or Helpdesk personnel are not responsive, requester may contact the next level of management to expedite resolution.

Escalation levels:

Level 1- Normal – Helpdesk Staff
Level 2- Escalation – Helpdesk Official

e) System Change Request Log

The helpdesk maintains the System Change Request Log. This log contains a consolidated list of all System Change Request Forms and the status of each request. The helpdesk continuously logs and updates the System Change Request Log throughout the approval and execution phases. The consolidated list of all System Change Request Forms will be located at a designated location known to IT official and Local Government Unit General Official.

f) Help Desk Post Service Follow-Up

After the service support has been implemented and tested, the following applies:

1. The Helpdesk will ensure the completion of the service support;
2. The Helpdesk will update the Log and file all documents.

f) Checklist

The following entries of a Service Support Record are investigated for their integrity and

completeness during the closure of the Service support request:

1. Protocol of actions
2. Person in charge
3. Support Group
4. Time and Date
5. Description of the activity
6. Documentation of applied workarounds
7. Documentation of the root cause of the Service interruption
8. Date of the Incident resolution
9. Date of the Incident closure

g) Scheduling & Communication

1. The Helpdesk will enter all Service Support requests on the Log to track and communicate scheduled change events to business units and IT.
2. The Helpdesk will send an informational email notification to the affected departments and/or external offices written by the Requester (with the assistance of the Implementer as needed).
3. System changes will normally be scheduled to minimize user/customer impact. Once any type of change has been scheduled and approved, the date and/or time cannot be modified.
4. A rescheduled Change must obtain authorizations of the individuals who signed on the original change request.
5. General notifications are sent by the helpdesk on as need basis such a plan for service interruption after being approved.

h) Reporting and Performance

Reporting is an important element of the helpdesk operation. It's a tool that provides management and helpdesk staff with an accurate measurement of IT activities and during the initial stage of implementation, will, allow the establishment of productivity baseline. Additional benefits of reporting include;

1. Identify weak links.
2. Provide management with metrics to assess the overall operation.
3. Up-to-date status on all projects and service requests.
4. Provides unified services and service request processes across the entire organization.
5. Provides statistical and trend reports to identify problem areas.
6. Improved service offering; Productivity; Open and close tickets; Tickets outside the SLA; Service request logging process.
7. Create project accountability.
8. Identify recurring trouble issues.

i) Type of Reports

The reports will include statistical data including; all open and closed requests by category, group, date, department, due date, level, priority, status, technician, status by level, status by priority, status by technician.

Major Incident Reporting and Notification

1. Incident reporting is handled by the Helpdesk after or during incident management.
2. If an incident occurs, the department or employee handling the incident is responsible to ensure that an "Incident Report" is completed and documentation is submitted to the helpdesk.

3. The Helpdesk will notify senior management and in some cases a notification will be sent to the Council in accordance with this policy and **Change Management Policy**.
4. If a major service such as Local Government Unit server is down more than # of minutes (60 minutes for example) or recurrence more than 1 time within 3 months if less than 60 minutes, then notifications will be sent to the Mayor and General Official.
5. If a system failure happens but doesn't affect core operation such as file or printer server, there is no need to notify senior management. However, an incident report will be created and sent to IT officials.

j) Incident Notification Policy

Severity	Systems or Services Affected	Down Time	Notification
High (2)		< = 30 Minutes	Not Applicable
Critical (1)	Key service is down such as (an example), main server where data were failed devices under Local Government Unit's control	>= 60 Minutes or recurrence more than 1 time within 3 months if less than 60 minutes	Mayor and GM

Report Intervals (or as seen fit by Management)

- Daily or weekly reports for IT departments
- Monthly reports for Local Government Unit's General Manager
- Quarterly reports for Mayor and Council

3.10.2.8 Knowledgebase

This module serves the helpdesk team as well as Local Government Unit system's users. Users can search the knowledgebase sections for solutions on basic issues such as connecting to a printer or a network resource. Also, when support staff employees resolve issues, they can directly convert these resolutions as knowledge base articles. Advantages of the knowledgebase includes: Efficiently respond to repeat issues, cut down support requests, allows end-users to search in Knowledge Base articles before submitting a ticket.

3.10.3 Hardware and Software Specifications

IT must identify the types of systems they have and according to the IT Purchase Policy, each unit must have a tag number or identification number.

3.10.4 Related Policies

1. Change Management Policy.
2. Disaster Recovery Policy.
3. Risk Assessment Policy.
4. Backup Policy.
5. Password Policy.
6. Vendor Management Policy.
7. IT Outsourcing Services Policy.

3.11 Data Backup Policy

3.11.1 Introduction and Goals

3.11.1.1 Policy Statement

The primary objective of this policy is to provide a comprehensive protection for the Local Government Unit's data. This policy seeks to outline the data backup and recovery controls for Local Government Unit's employees so as to ensure that the data is correctly and efficiently backed up and recovered in line with best practice. It aims at standardizing the backup methodologies used to improve the integrity of the hosted systems and the safekeeping of the data.

3.11.1.2 Scope

The policy applies to every individual using or interacts with the Local Government Unit's IT infrastructure, including third parties, service providers and consultants. This policy covers all information systems environments operated by the Local Government Unit or contracted with a third party. The Local Government Unit is the sole owner of all electronic information residing on any departmental computer system and per **the e-mail policy,** Local Government Unit's management may peruse, monitor and take copies of any information or communication made or received utilizing any of the aforementioned systems.

3.11.1.3 Purpose

This Data Backup Policy has been created to guide and assist the Local Government Unit to align with internationally recognized best practices to support and sustain the effective control of electronic data backup and to enable recovery of data in case of events such as system disk driver failures, data entry errors or natural disasters. It is regarded a crucial element in the effective protection of the Local Government Unit 's data and its IT systems.

Implementation of this policy helps to:

1. Address the risk of losing data;
2. Safeguard the confidentiality and integrity of information contained within the IT systems;
3. Guarantee "Business Continuity" through the immediate usage of the important data retrieved by recovery.
4. Define controls to enforce regular backups and support activities, so that any risks associated to the management of data backups and recovery are mitigated.

3.11.1.4 Responsibilities

1. IT department is the main section at the Local Government Unit responsible for the safety of the electronic data.
2. Local Government Unit's IT department official is responsible for supervising the implementation of this policy.
3. IT official must delegate two employees (one primary, one secondary) to commit and adhere to each backup schedule.
4. IT official will authorize a limited number of employees to access backups.
5. The Local Government Unit's council (or a specialized subcommittee) is responsible for reviewing, auditing and approving any changes (on annual basis).
6. It is the responsibility of each official, unit head and employees to ensure that use of the Local Government Unit's data complies with the guidelines as set out in this policy.
7. It is the responsibility of each employee to carefully adhere to the protocols of this policy to ensure the full safety of the Local Government Unit data.
8. It is the duty of the user (with the help of Help Desk) to ensure that all work-related documents are restored on the file server under his/her allocated directory.
9. IT official must ensure that all back-ups are successfully completed. In addition to backing up departmental data, IT department shall perform regular disk capacity management on all data servers and have the right to delete all non-departmental related data after consultation with involved employees.
10. IT official must monitor the status of all backups that are performed and any faults identified must be rectified.
11. IT official and IT staff must ensure that a backup is made by each employee before and after installing batches or upgrades or making any configuration changes on the system. This may be achieved using a combination of image copies, incremental backups, differential backups, transaction logs or other technique.

3.11.2 Policies and Procedures

3.11.2.1 Identify critical data

IT department must define "Critical Data" essential for the continued operation of the Local Government Unit which must be maintained by means of full and periodic back-ups and taken off-site to a secure location to enable the recovery mechanisms (as stipulated in the **Disaster Recovery Policy**). Data to be backed up include the following:

1. Users' data stored on the file server in each user's allocated directory;
2. All data and software relating to the continued operation of the Local Government Unit applications, information and configuration must be backed up regularly including:

a) Exchange Server and all Emails.
b) Mailboxes.
c) System state of all servers including PDC & BDC, WSUS, Mail Server.

3.11.2.2 Omitted data

IT department may decide to omit from backups specific file extensions such as Audio Video Interleave "AVI" extension or a Digital video and movie file type "Mpeg" extension or MP4 type files or others as seen necessary.

3.11.2.3 Encryption of Backup

IT must encrypt all Backup data to maintain Data confidentiality and integrity, and to prevent unauthorized individuals from using it.

3.11.2.4 Backup facilities

1. Local Government Unit should have its own backup storage facilities at its grounds;
2. Backup media must be stored off-site, at an environmentally-protected and access-controlled site, at a sufficient distance (suggested 6 km) to escape any damage from a disaster at the main site or for a long-term storage, together with accurate and complete records of the back-up copies and documented restoration procedures.
3. It is advisable to use appropriate storage medium such as a **cloud-based backup** to properly secure and archive critical data. The backup medium may include data replication or a mirrored server at a remote site (with a direct connection with the main server if possible);
4. Backup may be done manually through a disk, CD, tape, external hard drive, or any other recognized medium.
5. Adequate back-up facilities must be provided to ensure that all essential business information and software could be recovered following a disaster or media failure. A full checkup of the Local Government Unit assets will help discover the Gaps and must be included in the IT plan (#-years) as stipulated in the **IT Purchase Policy.**
6. Backup media that may be transported from the Server Room to the offsite storage location must be logged.
7. The on-site backup media log must contain the following information:

a) Date of taking the backup
b) Date of transporting the media to the offsite storage location
c) Contents of the media (e.g., transaction backup, application backup, entire system backup)
d) Nature of backup (e.g. full image copy or file copy)
e) Name of the Carrier

f) Name of the off-site storage location
g) Name and signature of the responsible person at the onsite location
h) Any other label information

3.11.2.5 Frequency of backup

All data and software must be backed up regularly according to an approved backup schedule (Manual or automated) that could be based on Incremental and Deduplication methods. Refer to the below example of backup-Schedule.

3.11.2.6 Backup schedule

1. A full backup should be run weekly and should be stored off site.
2. Differential/ Incremental backups must be done on daily basis.
3. Back-up arrangements for individual systems and related data must be tested according to a formal schedule to ensure that they meet the requirements of the **Local Government Unit 's Disaster Recovery Plan.**
4. IT department might consider taking full images of the servers as a backup to ensure that the system can be recovered with minimal knowledge of the system configuration. Furthermore, it is strongly advisable to standardize its backup solution and backup medium across all sites to implement the policy.

The following is a suggested schedule to follow for the IT department (which can be altered to create a form that fits better with the types of backups they are currently using or wishing to use):

	Monthly	**Weekly**	**Incremental**	**Validation Times**		
Servers	**All Hard Disks (full backup)**		**Daily Times**	**Weekly (Friday)**	**2nd Validation - Saturday**	**2nd Validation Sunday**
PDC	C,D					
BDC	C					
MIS-Server	C					
EDMS	C					

Exchange	C					

7.2.7 Automatic vs. Manual backup

Despite that Automatic and Manual backup procedures are in line with best practices, this policy recommends automatic backups (triggered by a program at certain intervals); however; IT official must carefully revise and monitor the schedule to include any non-standard updates and/or changes to the work schedule.

3.11.2.7 Recovery of Data tests

1. As stipulated in the **Disaster Recovery Policy**, operational staff must regularly test the backup/archive tapes to ensure that the tapes can be read and can be relied upon for emergency use when necessary. If normal procedures do not use backup tapes for restores on a fairly regular basis, then routine random tests should be performed at least weekly.
2. Backup recovery must be tested when any change that may affect the backup system is made. The Incident register information generated from each backup job will be reviewed daily for the following purposes:

a. Checks and corrects errors.
b. Monitors the duration of the backup process.
c. To improve backup performance where possible.

3.11.2.8 Backup Retention

1. Backups of all data must be retained such that all systems are fully recoverable. At a minimum, yearly backup must be retained for at least 5 years (dependent on the Local Government Unit capabilities)
2. All archival back-up data stored off-site must be reflected in an up-to-date directory which shows the date when the information was most recently modified as well as the nature of the information.
3. All media stored for periods longer than six (6) months must not be subject to rapid degradation.

3.11.2.9 Backup Documentation

1. Backup documentation must include identification of all critical data, programs, documentation, and support items that would be necessary to perform essential tasks during a recovery period.
2. Each backup media must be appropriately labelled with details of identifying criteria, date,

nature of backup (e.g. Full image or incremental). In addition, it must be given a classification label, as determined by the Local Government Unit. The following is the minimum identifying criteria for backup media:

a) Server name
b) Description of the Contents
c) Creation Date
d) Sensitivity Classification (based on applicable electronic record retention regulations).
e) The Local Government Unit contact information.

3. Backup and recovery documentation must be reviewed and updated regularly to account for new technology, business changes and migration of applications to alternative platforms.
4. Backup media not in use any longer must be securely disposed of, rendering the data on it unreadable.

3.11.2.10 Data Backup Standards

1. Update plans for systems and processes;
2. Sensitive Backup Data must be encrypted;
3. Storage infrastructures must use protection mechanisms to guard against all possible threats such as:

a) Unauthorized accidental or intentional corruption, modification;
b) Destruction of data or damage or loss of computers and hard drives;
c) Accidental deleting of files or formatting drives.

4. Third party vendors – if contracted to provide cloud computing storage for example - should be able to provide a 24x7 support services in case incidents happen outside the normal business hours;
5. Proper access controls should be used to prevent unauthorized access to the sensitive data stored in a third-party cloud environment including cloud service provider personnel **(see detailed access plans in Vendor Management policy and IT security policy)**.
6. Access to the backup media should be according to the data's classification and the user's job and role.

3.11.3 Related Policies

1. IT Purchase policy
2. Data Recovery Policy
3. Risk Assessment Policy

3.12 IP Addressing Policy

3.12.1 Introduction and Goals

3.12.1.1 Policy Statement

It is the responsibility of each Local Government Unit to protect its network infrastructure, systems, and data. The larger the networks, and the more services provided through them, make it more difficult protect the network, and this urges more investment, better management and continuous mentoring of network traffic. This policy provides the basis for directing network and IP procedures and practices within the Local Government Unit.

3.12.1.2 Scope

This policy sets out the requirements, roles and responsibilities for a secure Local Government Unit's network. And it provides the direction and basis for IT in the following areas:

1. Ensure, where reasonably practicable, that the network supports the full range of Local Government Unit activities and businesses, and allows the services effectively.
2. Ensure availability of electronic services.
3. Protect the Network from unauthorized access.
4. Protect the Network from accidental disruption.
5. Protect confidentiality.
6. Design, plan, manage, and control security on the network.
7. Manage access on the network and the electronic resources.
8. Log network access and activities, and ensure network access can be audited.

3.12.1.3 Purpose

Improve the administration and management of network protocols and security in order to minimize the risks of system faults, weaknesses, vulnerabilities and attacks.

3.12.1.4 Responsibilities and Roles

1. IT network and systems team:

a) Define appropriate user groups and roles to support Role-Based Access Control.
b) Audit users and access lists on a regular basis to ensure that unauthorized attempts are identified and for anomalies in Super User access.
c) Perform annual policy and procedure reviews.
d) Create and maintain procedures, and document all necessary network and network security configurations.

e) Monitor and analyze network traffic for optimum performance and security.

2. All Network Users:

a) Act responsibly at all times and be aware of the associated risks for breaches of this policy, including potential disciplinary processes.

3. IT Official:

a) Approve the policy and follow up on setting projects and procedures in order to comply with this policy.

4. General Manager of the Local Government Unit:

a) Final approval of the policy.

3.12.2 Policies and Procedures

3.12.2.1 Network Segmentation and Segregation

1. Network segmentation should be determined based on system function and the sensitivity of the data the systems store, processes and transmits. For example, the systems that require a connection to the Internet should be placed into a demilitarized zone (DMZ) that is separated and segregated (isolated) from more sensitive systems.
2. Server's networks should be separated from users' networks.
3. Database servers should be placed in a separated zone from the front-end application servers using multitier architecture. VLANs may be used to further separate systems and users' groups, which will provide more efficient protection.
4. Network segmentation and segregation will improve network performance, security, and minimize the impacts of risks like human made faults.
5. It is recommended that groups of information services, users, and information systems are segregated on networks. The following recommendations of ISO 27001 and ISO 27002 should be implemented at least:

a) Divide large networks into separate network segments;
b) Consider physical and logical segregation;
c) Define segments perimeters;
d) Define traffic rules between segments;

e) Use authentication, encryption, and user-level network access control technologies;
f) Consider integration of the organization's network and segments with those of business partners.

3.12.2.2 Network Design

Consider the following concepts in network design:

1. **Classification:** Classified systems should be segregated (refer to the digital security policy for classification).
2. **Security Zones:** A security zone is a group of one or more physical or virtual firewall interfaces and the network segments connected to the zone's interfaces. Protection for each zone is individually specified and controlled so that each zone receives the specific protections it requires according to classification, endorsement, compartment and sensitivity of data.
3. **IP Address Management:** A well-structured IP addressing scheme promotes the ability to quickly identify node properties from an IP address which assist in:

a. network management and fault finding and rectification.
b. Defined network perimeters and boundaries;
c. Defined network traffic rules.

4. Internal IP address ranges are defined by the network and systems team.
5. DHCP should be used for allocating dynamic IP addresses for users' PCs and peripherals.

6. Connector Types and Cable Colors: There should be separation of electrical and electronic circuits, devices, equipment cables, connectors and systems.

7. Central Information Repository:

IT should create a central repository of all the information on networks, IP addresses, protocols and devices, this is critical to maintain control of the network. This will be single repository where all the data relevant to networks, hosts, servers, dynamic clients, and virtual environments can be tracked and audited. The ability to search across all this information will enable network teams to quickly track changing network landscapes and rapidly troubleshoot issues as they arise. In addition, business data related to a network resource helps bind together the logical network construct and the reality of IT resources.

8. Risk Assessment:

Risk assessment should be fundamental tool in the architecture and design of a network, Risks should be identified, analyzed, assessed, and controlled through risk management techniques.

9. Security Architecture:

All security requirements should be considered in the network design and architecture including the principles of network segmentation and segregation as well as the system classification. The security architecture maximizes the design and operational efficiency and provide and support essential security requirements of the network design.

10. Classifications and categories of network segments

Classification of systems is essential for all architecture and design elements and systems documentation. Different IP addressing schemes should be used for the segments with access lists controls between the different networks, firewall protection should be implemented between the different network zones. Effective security controls should be conducted between networks.

11. IP telephony

Private IP addresses should be assigned to IP phones, because they don't require direct internet connectivity.

3.12.2.3 Physical and environmental network security

1. All core network switching, management systems and port distribution systems will be housed in a secure location with UPS and access control.
2. These secure areas will:

a) Allow entry to secure areas with critical or sensitive network equipment only to those who are authorized to do so.
b) Have secure code or card access systems.
c) Only allow visitors or 3rd party access with authorization. A list of authorized users will be maintained and regularly reviewed.
d) Will not allow smoking, eating and drinking in these spaces is prohibited.

3. Before any visitor or 3rd party is provided access to secure network areas, agreement to all relevant Policies should be signed and will be made aware of security requirements.
4. All visitors to secure network areas must be logged in and out. The log will contain name, organization, purpose of visit, date, and time in and out.

3.12.2.4 Access control to the network

1. Access to the network will require a secure log-on.

2. Registration and de-registration procedure for access to the network will, in the first instance, be driven from the HR System to create employee/staff. Separate authorization will be required for remote access to the network.
3. Access rights to the network will be allocated on the requirements of the user's job, rather than on a preference or perceived need.
4. Similarly, security privileges (i.e., 'Power user' or network administrator rights) to the network will be allocated on the requirements of the user's job. A list of which will be securely maintained and reviewed regularly.
5. All users to the network will have a unique user identification and password.
6. Users are responsible for ensuring their password is kept securely and not shared with others (see the digital security policy).
7. User access rights will, upon notification from the HR, be removed or reviewed for those users who have left the Local Government Unit.

3.12.2.5 Firewall standards

1. A firewall is defined as any hardware and/or software designed to examine network traffic using policy statements (rule set) to block unauthorized access while permitting authorized communications to or from either a network or electronic equipment.
2. All network (physical) firewalls installed and implemented, must be implemented or overseen by the Network and Systems Team.
3. All firewall modification requests must be logged in the Service Desk call logging system.
4. All changes to firewall rule sets should be documented and recorded.
5. All related documentation is to be retained by the Network and Systems Team and it is subject to regular review.
6. All firewall implementations must adopt the position of "least privilege" and deny all inbound traffic by default (the initial rule set should be set to "logging or learning mode" to prevent service interruptions). The rule set will only be opened incrementally to only allow permissible traffic
7. Firewalls must be installed within production environments where "Legally/Contractually Restricted Information" is captured, processed or stored, to help achieve functional separation between web-servers, application servers and database servers
8. Firewall rule sets and configurations require annual review to ensure they afford the required levels of protection.
9. Network and Systems Team must review and agree all network firewall rule sets and configurations during the initial implementation process.
10. Firewalls protecting the Local Government Unit's systems must be reviewed twice a year.
11. Firewall administrators must retain the results of firewall reviews and supporting documentation; all results and documentation are subject to regular review.

12. Firewall rule sets and configurations must be backed up frequently to alternative storage (not on the same device). Multiple generations must be captured and retained in order to preserve the integrity of the data. should restoration be required. Access to rule sets and configurations and backup media must be restricted to those responsible for administration and review.

a) Wired network

- Only the Local Government Unit's owned equipment may be connected to the wired Network. This includes network services supplied to all buildings.
- Personal laptops are not eligible for wired network connections without formal requests that is logged and supported by IT. The Local Government Unit will provide wireless networks, which are for mobile computing connectivity including; laptops, mobile phones and smart devices.
- Use of network addresses other than those provided by IT is prohibited.
- Access to networking equipment in data centers and communications rooms is limited to IT staff and authorized personnel only.
- Only one device may be connected to any physical wired network port. No hubs, switches, wireless access points or routing devices may be connected, directly or indirectly, without prior agreement from IT.
- Network and Systems team has the right to limit network capacity or disable network connections that are affecting available network bandwidth to the detriment of the Local Government Unit. Where possible, and depending on the severity of the incident, this will be done in negotiation with the impacted units of the Local Government Unit.
- No individual may connect a device to the Local Government Unit's wired network that provides unauthorized users access to the network or provides unauthorized IP addresses for users.

b) Wireless network

The Local Government Unit should establish a secured and hidden wireless network across its buildings for use of its staff. Another secured wireless network is made available for visitors that is completely separated from the Local Government Unit's network. The wireless networks' security standards are as follows:

1. Access Layer: users will connect to the WLAN via access points, which will provide the 802.11g/n connection standard for the client devices.

2. Service Set Identifier the SSID for the wireless networks of the Local Government Unit will be identified by IT and it will be in the format of "Local Government Unit name"-Private for staff network and "Local Government Unit name"-Visitors for the visitors.
3. The Network and Systems team may provide service providers access to the staff wireless network if that is required to enable service support.
4. The WLAN networks will utilize AES (Advanced Encryption Standard) level of encryption. This encryption standard is mandatory.
5. The WLAN networks service supports only WPA2 (Wi-Fi Protected Access) which is the preferred security standard.
6. Unauthorized devices connected to the wireless network will be blocked without warning.
7. Staff are prohibited from connecting additional wireless network hotspots to the Local Government Unit network.

c) Third party access control to the network

1. Third party access to the network will be based on appropriate authorization and compliance with all relevant policies.
2. IT team are responsible for ensuring all third-party access to the network is recorded.
3. Access to the internet may be provided for Local Government Unit staff, visitors or contractors, service providers via help desk.
4. Connection to the Local Government Unit's Wi-Fi staff infrastructure may be approved where the appropriate request is made in writing to establish a named account or the appropriate self-registration process is undertaken.

d) External network connections

1. Connections with external networks is allowed based on business requirements after getting request from business department\s, IT will get the request, analyze, agree with the department on connection requirements, then it send its recommendations to the general official for final approval.
2. IT is responsible for implementing all connections to external networks that connect to the primary Networks, ensuring that related systems and networks are compliant with laws, regulations, and approved policies.
3. IT is responsible for logging and auditing the external connections, with periodic review of the connection requirements.

3.12.2.6 Network maintenance and backup

1. Network and systems team will ensure that maintenance contracts are maintained and regularly reviewed for all essential network equipment.
2. The Service Desk is responsible for ensuring that a log of all faults on the network is maintained.
3. Networks and Systems team will ensure a log of current network and switch configurations. Changes will be maintained and stored securely and backups of switch configurations taken regularly. The Network and Systems Team will:

a. Document procedures for the backup process and ensure that it is communicated to all relevant staff.
b. Document procedures for the storage of backup tapes or media will be produced and communicated to all relevant staff.
c. Ensure all backup media will be stored securely and a copy will be stored offsite.
d. Document procedures for the safe and secure disposal of backup media will be produced and communicated to all relevant staff.
e. Users are responsible for ensuring that they backup their own data to the network server using mapped drives.
f. Network patches and any fixes will only be applied by the Network and Systems Team following a suitable change management policy.

3.12.2.7 Protection and malicious attacks

1. The Network and Systems Team will ensure that:

a. Measures are in place to detect and protect the network from viruses and other malicious software.
b. They have suitable monitoring of network traffic, network access and intrusion detection in place.
c. The network will be monitored for potential security breaches. All monitoring will comply with the laws, regulations and approved policies.

2. IT department reserves the right to access, modify or delete all data stored on or transmitted across the Local Government Unit's network as part of defending the network and digital security requirements. This includes data stored in personal network folders, mailboxes etc. Data of a personal nature should be stored in a folder marked or called 'Personal'. This does not preclude access or removal of such a folder on the authority of the IT.

3.12.2.8 Simple Mail Transfer Protocol (SMTP)

1. All email protocol traffic shall utilize the centralized mail gateways. Inbound mail traffic with destination addresses for servers other than those operated by IT Services shall utilize a DNS MX record to relay that traffic through the centralized mail gateways. All outbound traffic shall utilize the SMTP gateway.

2. The use SSL or TLS based communication standards for email client to email server communication is preferred such that the authentication session is the protected transaction.

3.12.3 Related Policies

1. Helpdesk Policy
2. Information Security Policy
3. Risk Management Policy

3.13 IT Staff Hiring Policy

3.13.1 Introduction and Goals

3.13.1.1 Policy Statement

This policy is established to ensure enough resources are hired (directly or indirectly) as part of Information and Communication Technology "IT" department assets. IT assets are made of systems ((hardware and software), and human resources who are the crucial element behind the success of the operations and services to citizens. The needs of the IT department should be included in the Local Government Unit annual plans as stipulated in the **Assets Purchase Policy**. A clear management structure for the IT department with defined job roles must be approved by the Council to be included in the Local Government Unit management structure; hence, related costs will be included in the Local Government Unit budget.

3.13.1.2 Scope

This policy applies to all employment positions within the IT department at the Local Government Unit. Enough resources must be contemplated to allow the safe delivery of these goals:

1. Improvement in overall productivity and performance of Local Government Unit;
2. Achievement of greater efficiencies;
3. Realization of positive Returns on Investments (ROI) in technology.

3.13.1.3 Purpose

The policy establishes standards to ensure hiring and maintaining a competent and qualified workforce at the IT department based on defined criteria and procedures that the Local Government Unit will utilize for establishing positions, recruiting, selecting, and hiring employees. It will be done in a fair equitable manner.

3.13.1.4 Policy Statements

1. Council to study and approve budget funding for all new permanent employee positions that are established by the Local Government Unit that require additional funds.
2. The IT Department official is permitted, under the supervision of the HR department, to utilize all established and funded permanent employee positions. Additionally, the IT Department Management shall have officially discretion in utilizing "Temporary Employees" and contracted services provided all relevant costs are incurred within Council approved budgets.
3. The IT Department official and HR department shall be the Local Government Unit representative authorized for the hiring, appointing, disciplining of the employees in the IT department.

4. IT Department Official will determine if vacant positions, both permanent, temporary and casual will be filled and initiate the posting process with Human Resources.
5. Dismissal of employees is a joint decision between HR and IT departments taking into consideration the relevant Palestinian labor laws;
6. Normal staff structures should be designed to accommodate for most events in the daily activities of the IT department. It is however acknowledged that there are times and situations where temporary personnel may be used.

3.13.1.5 Responsibilities

1. IT department senior official is responsible for developing the IT plan and to submitted to the Local Government Unit Council for approvals;
2. In case, no IT department exists, the Council must create an IT Committee to lead the process and take over the responsibilities of the IT department official and implement this policy;
3. Finance Department is mandated to include the Council's decisions in the budget;
4. Human Resources department are mandated to hire the needed resources.

3.13.2 Policy and Procedures

3.13.2.1 Policy Statements

1. Council to study and approve budget funding for all new Permanent Employee positions that are established by the Local Government Unit that require additional funds.
2. The ICT Department Manager is permitted, under the supervision of the HR department, to utilize all established and funded Permanent Employee positions. Additionally, the ICT Department Management shall have managerial discretion in utilizing Temporary Employees and contracted services provided all relevant costs are incurred within Council approved budgets.
3. The ICT Department manager and HR department shall be the Municipal representative authorized for the hiring, appointing, disciplining of the employees in the ICT department.
4. ICT Department Manager will determine if vacant positions, both permanent, temporary and casual will be filled and initiate the posting process with Human Resources.
5. Dismissal of employees is a joint decision between HR and ICT departments taking into consideration the relevant Palestinian labor laws;
6. Normal staff structures should be designed to accommodate for most events in the daily activities of the ICT department. It is however acknowledged that there are times and situations where temporary personnel may be used.

3.13.3 Standard requirements process framework

3.13.3.1 Identify the human resources needs

IT Department senior official must adhere to the results discovered in the "gap analysis" as stipulated in the **IT Assets Purchase policy** which details current assets of the IT department and which elements are missing and how to compensate it. Objective planning requires annual revisions of the IT department plans which must be a rolling number (#) year plan.

3.13.3.2 Qualification and experience requirements

Based on the results of the IT plan, the senior department's official must design the job role according to the following:

1. Specialized experience needed to handle the job versus general knowledge;
2. Number of years of experience in the same field;
3. Level of education needed to do the job;
4. Special certifications needed to handle the job;
5. General Industry knowledge in the field he/she will work within;
6. Other related skills such as the communication and team skills;
7. Assign Salary and related benefits (based on the Local Government Unit approved Salary scale).

3.13.3.3 Announcing Vacancies

a) Vacancies for positions will be posted on the Local Government Unit 's website and/or in local newspapers, recruiting websites (jobs.ps as an example), and through professional associations.
b) Vacancies will be posted for at least 10 days unless it is a senior position it will be posted continuously for at least 15 days
c) The announcement will include minimum requirements in terms of skills, expertise and other qualities for appointment. Also included, a summary of the key performance areas/primary duties of the position and a clear statement declaring that the appointment will be permanent or for a fixed term, and the term (if applicable).
d) If there are no suitable candidates, job postings may be extended as required.

Exceptions:

All position vacancies will be posted, and an employment competition will be held in accordance with this policy unless:

1) As part of **Succession Planning**, at the discretion of the Local Government Unit General Official, an internal employee currently employed with the Local Government Unit with good performance reviews may be appointed to a senior role without the need to post the position providing they meet the qualifications of the senior role, such as an official moving to a director role.
2) No need to repost a position if it was filled but the candidate or the Local Government Unit terminated the contract in the first three (3) months of hiring. The Local Government Unit may, in accordance with the applicable provisions of this Hiring Policy, offer employment to other qualified applicants instead of re-posting the vacancy.

3.13.3.4 Local and Internal Hiring Considerations

The Local Government Unit encourages local and internal hiring through the following policies and practices:

a) Local job advertising requirements (in local newspaper) ensure the visibility of postings to the local community;
b) Council may decide to give 10% additional marks to applying candidate who lives within the Local Government Unit jurisdiction;
c) Internal applicants for an announced job adhere only to the level of experience and /or ability to do the job, his/her overall conduct and should be recommended by the IT official;
d) HR will designate the internal applicant as qualified and include the employee's name on the master list of candidates; however; being an employee does not make him/her the winner of the job;
e) Hiring Committee should carefully study the employee profile to make sure that he/she can deliver the tasks required.

3.13.3.5 Interviewing

1. Except for appointments that must be made by the Council, the Mayor will assign a selection committee made from HR official or an employee of the department, IT department senior official and the Local Government Unit general official;
2. After the closing date of the job advertisement, Human Resources will prepare a master list, in a table format, detailing:

a. Applicants Name
b. Applicants' qualifications and experiences relevant to the Job description
c. A copy of his/her CV should be maintained ready to be reviewed by the selection committee if requested

3. HR department will invite all qualified applicants (screened against appropriate criteria established from the job qualifications set out as required in the job description) attend an interview;
4. Answers will be ranked according to the skills required. Interviewers will document applicants' answers to questions to assist in the evaluation of each applicant's qualifications.
5. All interviewees will be asked the same questions and ranked using the same system
6. All interviewees will go through a skill test to validate their abilities to perform the duties listed in the job description.

3.13.3.6 Selection

1. The selection team shall strive for consensus when recommending a candidate for hire to the Local Government Unit General Official who shall make the final hiring decision. Where consensus is not possible, the General Official must be in approval for the selection as well as the IT department senior official.
2. Interviewed unsuccessful applicants will be informed by email.
3. Feedback will be provided to unsuccessful applicants if requested. Such feedback will be limited to the job-related factors that impacted the selection decision.

3.13.3.7 Hiring

All employment offers are conditional on a candidate:

1. Supplying all employment-related documentation the Local Government Unit may reasonably request.
2. Executing a written employment contract with the Local Government Unit before their employment commences.

3.13.3.8 Training

The IT Official must ensure that resources are allocated and used in accordance with IT asset management General Instruction and that training is conducted according to IT user-staff training.

3.13.3.9 Conflict of Interest

Any individual who has a conflict of interest as stipulated in this policy must report it to the selection committee to study if there is a need to replace that member and the extend, he/she affects the decision to hire which may result in any actual, potential or perceived conflict of interest in the hiring process. No individual involved in the hiring process may use his/her power in his/her own interest or the interest of a third person or place himself/herself in a situation of conflict or potential conflict between his/her personal interest and his/her duties regarding this policy.

3.13.3.10 Nepotism

Careful consideration should be taken if a job candidate will serve in a position where their direct supervisor or subordinate is a direct family member. In particular, it is prohibited for family members of the Council to be hired in a position where there direct reporting relationship is to the Council. Also, if a family relationship develops that puts members of Council or employees in a direct reporting relationship, the individual(s) involved must inform the Council immediately to address this matter in a fair and equitable manner. All decisions made to remedy the situation must be documented with the Human Resources department and kept in the employee file.

3.13.3.11 Confidentiality of the Hiring Process

All personal information of candidates or applicants in the custody of the Local Government Unit, for example CVs or any other related information, is subject to full protection and should not be distributed outside the Human Resources department and the selection committee and only as part of screening process. In the case of announcement of a successful candidate, only his/her name and position will be announced (No other personal information and qualifications will be disclosed).

3.13.4 Related Policies

1. IT Assets Purchase Policy

3.14 Mail Policy

3.14.1 Introduction and Goals

3.14.1.1 Policy Statement

This policy is established with regard to access and disclosure of internal and external electronic communication messages (e-mail) created, sent, received or stored, via the internet or the Local Government Unit's intranet, by its employees, officials, heads of departments, visitors and contractors using the Local Government Unit's e-mail systems. It is the responsibility of each official, unit head and employees to ensure that use of the Local Government Unit's e-mail system complies with the guidelines as set out in this policy. As such, the Local Government Unit will take reasonable steps to protect confidential and restricted information that is created, received, transmitted and stored by the Local Government Unit's email systems and messaging functions. The e-mail system is the Local Government Unit's property and thus all copies of messages created, sent, received or stored on the system are and remain the property of the Local Government Unit.

3.14.1.2 Scope

This policy applies to:

1. All Local Government Unit's electronic communication facilities.
2. All messaging functions including instant messaging.
3. All Local Government Unit's staff members using its electronic mail facilities, email systems or messaging functions to store or transmit information including general, confidential and restricted information.

3.14.1.3 Purpose

To protect the confidentiality, integrity, and availability of confidential and restricted information created, received, transmitted, and stored by the Local Government Unit electronic communication facilities or email systems and messaging functions.

3.14.1.4 Responsibilities

1. IT department is the main party responsible for the safety of the electronic communication messages.
2. It is the responsibility of each Official, Unit Head and employees to ensure that use of the Local Government Unit's e-mail system complies with the guidelines as set out in this policy.
3. It is the responsibility of each employee to carefully adhere to the protocols of this policy to ensure the full safety of the Local Government Unit information.

3.14.2 Policies and Procedures

3.14.2.1 Email Accounts

1. Only employees with a legitimate need will be granted access to Local Government Unit's networks or systems.
2. Whenever possible, access to the Local Government Unit's email system will be limited solely to the functions and data that are necessary for employees to fulfill their job responsibilities per the **Digital Security Policy**
3. All users are granted the use of one domain account or login. In addition, users may be granted the use of other application accounts on a need basis.
4. Access to these accounts must never be shared with any other users.
5. Each account must be unique to the individual user.
6. Per the **Password Change Policy**, accounts should equate to first initial and last name wherever possible.
7. Whenever a user quits their job at the Local Government Unit, their accounts must be immediately disabled.
8. The IT department official should conduct quarterly reviews of user IDs and privileges associated with an account in particular email user accounts.
9. Department officials must supply the System Administrators with a list of active accounts and associated privileges every quarter.
10. Where possible, applications should be integrated to Active Directory for the purposes of identity management and password provisioning.

3.14.2.2 Acceptable Use of Local Government Unit's Email System

The Local Government Unit issued electronic mail "email" accounts is provided to facilitate the business of the Local Government Unit. Hence; the Local Government Unit's email systems are intended for the sole use of the Local Government Unit's business, not for personal communication or other inappropriate activities.

Incidental, occasional personal use is permissible so long as:

1. It does not consume more than a trivial amount of system resources.
2. It does not interfere with the productivity of the individual (both sender and receiver).

3.14.2.3 Email Banner

A warning banner should be part of the email signature for all outgoing email destined to external recipients and should include a confidentiality notice with the intent to make clear to keep confidential any unpublic or privileged information the email may contain and to inform any recipient who receive the message in error about what actions to take. The banner is to be configured on the email server, when feasible, so users do not have to include the message as part of their personal email signatures.

3.14.2.4 Contractor Banner "Third Party resources"

To clearly identify email written by an authorized Third Party who is using a provisioned Local Government Unit's email account, a warning banner must be included in the email signature for all outgoing email to indicate that the email messages are originating from a non-Local Government Unit employee.

3.14.2.5 Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, users of electronic communications should exercise caution when forwarding messages. Local Government Unit's confidential information must not be forwarded to any party outside the Local Government Unit without the approval of an official. Blanket or automatic forwarding of messages to parties or mailboxes outside the Local Government Unit is prohibited. This includes automatic forwarding from one account to another and of Local Government Unit's IT department email to personal, and non-Local Government Unit's email addresses. The following must be considered when forwarding messages:

1. Automatic forwarding of email messages by Local Government Unit employee to their personal email addresses is prohibited.
2. Individual email messages containing confidential and restricted information must not be forwarded or disclosed to Local Government Unit's employee without a need to know, or to parties outside the Local Government Unit, or to other Local Government Unit offices unless there is a clear business need to do so and is permitted or required by law.

3.14.2.6 Secure Email Transmission Outside the Local Government Unit

1. Sending email messages containing "unpublic" confidential or restricted information to individuals or entities outside the Local Government Unit is allowable only to individual or personal email addresses that can be verified using reasonable measures as clarified by the **Password Change Policy.**
2. The Local Government Unit will encrypt transmissions of email messages containing electronic or unpublic information only when feasible and agreed upon by the Local Government Unit and the recipient.

3. All encryption solutions and tools for storing or transmitting email messages containing electronic or Local Government Unit's confidential and restricted information must be approved by the IT department.
4. If an encryption solution is not available, email messages containing unpublic information sent outside the Local Government Unit will be secured by other means (e.g., password protected and the recipient of the email should then be provided with the password by phone).
5. Efforts should be made to eliminate or reduce the amount of nonpublic information in any email. For example, list only a partial account number versus the entire account number so that the email is no longer classified as Confidential.
6. Employee must exercise reasonable care in addressing emails and instant messages appropriately so they are not inadvertently sent to incorrect addressees.

3.14.2.7 Use of Non-Local Government Unit Email Systems

Employees are strongly discouraged from using any non-Local Government Unit's communication systems. Use of Internet-based email systems as well as downloading attachments from these systems to Local Government Unit's systems could expose it to increased risk and harmful situations such as a virus or worm outbreaks or installation of a Trojan horse virus. Additionally, information stored on internet-based email systems is not secure and is sometimes scanned for content and keywords exposing the Local Government Unit to real threats.

3.14.2.8 Email Systems prohibitions

1. The unauthorized or otherwise inappropriate use, disclosure, modification, or destruction of designated "confidential information" that may or may not adversely affect the Local Government Unit is prohibited.
2. Impersonating another employee to access the email account holder or messaging function accounts is prohibited.
3. Employees are not authorized to retrieve or read any e-mail messages that are not addressed to them.
4. Employees shall not use any password or code, access a file, or retrieve any stored information, unless authorized to do so by an appropriate supervisor.
5. Falsifying a message's point of origin by altering any information that indicates the true source of the message.
6. The use of the Local Government Unit's email systems or messaging functions in a manner that violates the provisions of Local Government Unit's Information Security Policy.
7. The email and other information systems are not to be used in a way that may be disruptive, offensive to others, or harmful to morale. Any transmission or use of email that contains slurs or any message that may be construed as harassment or offensive to others is prohibited and could result in appropriate disciplinary action, up to and including termination.

8. The email system should not be used to engage with other people for reasons not related to their jobs such as for commercial ventures or political causes or other personal matters.
9. Email messages must not contain any material that may be considered offensive, disruptive, defamatory, or disparaging towards any employee, the Local Government Unit or Third Parties.
10. It is prohibited to use the email system in a way its violets any Palestinian law or other Local Government Units' related laws.

3.14.2.9 Email Retention

Palestine has no national record laws to enforce a specific time for retaining emails. However, it is highly advisable to follow a specific procedure to deal with these records based on its "value". Emails who fall into the following categories, may not be disposed of and must be retained if they**:**

1. Are evidence of Local Government Unit's transactions.
2. Approve an action, authorize an action, contain guidance, advice or direction.
3. Relate to projects and activities being undertaken, and external stakeholders.
4. Represent formal business.
5. Communication between staff; or Contain policy decisions.
6. If email communications contain data which can be considered part of a customer's record, the Local Government Unit's employee will retain the communications in the system record.

Otherwise,

1. In accordance with the Backup policy, Local Government Unit will automatically delete stored email messages in user accounts after a specific grace period of time approved by the Local Government Unit's council.

2. If email communications containing any Local Government Unit information need to be retained beyond the automatic email deletion period, Local Government Unit employee must save the messages by other means (e.g., archiving, copying and pasting into other documents, or printing out).

3.14.3 Related Policies

1. Digital Security Policy
2. IT Backup policy
3. Risk Management Policy
4. Password Change Policy

3.15 Device Naming Convention Policy

3.15.1 Introduction and Goals

3.15.1.1 Policy Statement

Protection of the Local Government Unit's data is the responsibility of everyone at the Local Government Unit. When the computers the data resides on becomes compromised or inoperative in some way, steps must be taken to locate the system to either repair it or to isolate it from the rest of the systems on the network until such time as the device is repaired or the compromise has been corrected. The Key to fixing the system is finding it, along with the respective user and those responsible for the maintenance. A standardized naming convention allows for positively identifying the computer.

3.15.1.2 Scope

a. All personnel responsible for managing departmental computing assets specifically desktop computers, mobile computing devices,
b. All personnel responsible for maintaining the confidentiality, integrity and availably of assets on the Local Government Unit's network.
c. This policy is mandatory for all new system purchases and will be applied with each system received and configured by IT department's technical personnel.
d. The standards in this policy are recommended and encouraged for all existing systems.

3.15.1.3 Purpose

The purpose of this policy is to help the Local Government Unit's IT department establish a standardized naming convention for IT assets that is scalable, readable, standardized and flexible and to allow those assets to be quickly and positively identified so they may be serviced and/or secured in a timely manner.

3.15.1.4 Responsibilities

1. IT department is responsible for implementing this policy.
2. Asset unit or whoever takes that role is responsible for ensuring that each IT asset has an Inventory Control number that must a have six digits at the end of it. For example: Name of Local Government Unit – 123456 or Name of Local Government Unit – XXX-123456.
3. IT will provide guidelines for implementing this policy if requested.

3.15.2 Policies and Procedures

3.15.2.1 Basic Structure

1. This policy establishes a basic set of criteria to define what information the hostnames must include to enable the **operations team** to read a device name and understand where the device is, what the device does, how critical it is, and what type of device it is.
2. Some systems have specific requirements for naming conventions. For example, Active Directory doesn't allow device names over 15 characters, and some systems have problems with special characters. In the following section, we'll make sure the name is valid with the system we suggest the Local Government Unit uses, taking into consideration that effective naming conventions is both practical and scalable.
3. **Instructions for Mandatory requirements:** To ensure interoperability with the Local Government Unit's records, we suggest that only letters and numbers to be used. Each IT asset name associated with this convention shall have the following structure:

a. **Mandatory requirement -The location (Ownership) of the device:** First three (3) characters of the appropriate department identifier (three-digit abbreviations) as the first three (3) Characters of the name (**mandatory**) such as the department name **acc** for accounting.

b. The next six (6) characters of the name (fourth through ninth positions) may be used at the discretion of the department, or not used at all (optional) such as:

I. The service level of the device (dev, qa, prod,) For example: acc-p;

II. The role of the device (web, database, mq) so now we have acc-pweb;

III. A two/three-digit sequential number [for dealing with multiple servers: acc-pweb01; or you may use the following abbreviations adapted from University of Waterloo:

- **DC**: Domain Controller
- **FS**: File Server
- **PS**: Print Server
- **ORA**: Oracle database
- **SQL**: SQL database
- **DB**: other database(s)
- **EXH**: Microsoft Exchange
- **CTX**: Citrix Server
- **ESX**: VMware ESX Server

The host names can include other information such as service name and device type (e.g. physical vs. virtual) that helps provide information about a device; Virtualization Review recommends the following:

- **V**: (Virtual)
- **C**: (Cluster server)
- **P**: (Physical)
- **O**: (Outsourced or vendor supported system)

c. The remaining six (6) positions should be the device's inventory control tag number (the last six characters of the tag number for example: Hebron-123456) (**mandatory**);

d. To improve readability of the device name, you may use a delimiter to separate the device location from its other specifics if the Local Government Unit's system allows it. **The standard delimiter** to separate the first part of the name (location, type, role) from the second part (unique ID) **is a dash: - and in** case Local Government Unit's system doesn't support a dash, you can use another standard character such as # or $ or simply disregard delimiters completely.

Example

Department – Accounting

Department ID – Acc001

Service level: Production

Role of device: web

Device type: Virtual

Inventory Control number: Hebron Local Government Unit - 123456

Acceptable names:

- Accpweb01-123456
- Acc00-123456
- Acc123456
- Accvir-123456

3.15.2.2 Process: New systems Process

When a purchased system arrives to the Local Government Unit, it will be delivered to the IT department to be configured with the appropriate disk image (operating system, image, etc.)

encrypted and joined to the Local Government Unit's active directory domain. As part of being on the domain, IT department will assign a name to the device and create the active directory account related to the device. To maintain consistency, all device names will include the full three (3) character department identifier and the six (6) numbers of the inventory control tag number where these names meet the standard spelled out in Mandatory requirements above.

3.15.2.5 Existing Systems Process

Renaming systems already in use at the Local Government Unit is encouraged. Those new names must meet the mandatory requirements described earlier (mandatory first three (3) and final six (6) characters) for both the device and the active directory account.

3.15.3 Related Policies

1. IT Purchase Policy
2. Information Security Policy

3.16 Media Policy

3.16.1 Introduction and Goals

3.16.1.1 Policy Statement

This policy was established to manage the official presence of the Local Government Unit on the Internet, represented by the Local Government Unit 's website, its application on mobile phones and other social media channels. The Local Government Unit 's online presence is an essential source of information accessible by the public and is a key tool to deliver timely news, programs and services. it is highly recommended that Local Government Unit social media accounts be linked to the Local Government Unit site (where possible) for the purpose of downloading forms and documents and providing specific information. The Local Government Unit is the sole owner of its website and any other social media accounts; hence, it will remain under the full control of the Local Government Unit regardless of any possible changes made in the Local Government Unit council or senior management, or third-party provider or Administrator.

3.16.1.2 Scope

This policy applies to all Local Government Unit employees and officials who make public statements on behalf of the Local Government Unit on its social media networks that discuss, share or comment on its news and activities. Also, it applies to the public who visit the different Local Government Unit 's social media channels and posts comments. It also applies to "Third parties" who has a contract with the Local Government Unit to handle (fully or partially) anything related to the Local Government Unit 's social media networks and it applies to all Local Government Unit media channels as defined in this policy.

3.16.1.3 Purpose

The purpose of this policy is to set guidelines and standards to ensure the appropriate use and management of social media on behalf of the Local Government Unit. Social media should be used as a communications tool for the intent of enhancing communication from the Local Government Unit to the public about programs and services for the following purposes:

1. Raising awareness and sharing information.
2. Recruiting volunteers and employees.
3. Promoting Local Government Unit events, programs, and services.
4. Increasing access to information for specific audiences.
5. Promoting opportunities for public involvement and comment on the Local Government Unit 's online engagement platform.

3.16.2 Policies and Procedures

3.16.2.1 Designated Responsibility

The Local Government Unit ’s senior management team is responsible for designating the role of Social Media Account Administrator. Where possible, a single staff person (preferred with public relations background and social media understanding) should be designated as the Social Media Account Administrator for each Corporate or Separate account owned by the Local Government Unit. This employee is responsible for posting, monitoring, and maintaining the account on behalf of the Local Government Unit, Department, or Committee. The employee is responsible for handling any third party who has a contract to deliver services in that regard. In addition to the regular Social Media Account Administrator, an alternate Administrator should be identified.

3.16.2.2 Account Creation & Management

Social Media Account Administrator need the approval of the senior management before creating either a corporate social media account or adding a new social media channel presenting the added value from creating the new accounts or channels. This is an important step as it might trigger the need to either hire or designate more people to handle the new accounts. Per the **IT Staff Hiring policy**, adequate resources including staff time (internally or externally) and material must be present as part of the decision-making process. Social Media Account Administrator must review any existing social media to ensure full compliance with this policy and review discoveries with senior management.

3.16.2.3 Account Administrators Responsibility

1. Social Media Account Administrator is acting on behalf of the Local Government Unit when he/she engages in social media activities so best judgment must be used when interacting with the public to ensure full compliance with the Local Government Unit ’s requirements and this policy.
2. Must not use corporate accounts to express personal opinions or further personal agendas.
3. Ensure proper protocols and permissions are obtained for posting any copyrighted material (including documents, websites, logos, images).
4. This policy applies on any external parties who has a contract with the Local Government Unit to do any job related to its social media as stipulated in the IT Purchase Policy.

3.16.2.4 Content Management - General Content

1. Account Administrator must keep the Local Government Unit accounts updated with new information when possible because long and frequent periods of inactivates (3-4 weeks) will lead to serious damage to the credibility of the Local Government Unit and the established communication channel.

2. Senior management must be informed and initiate discussions with department heads to ratify the situation including possibilities on the continuity of the channel.
3. Continued regular audits of the accounts is a must to ensure inappropriate postings are removed in a timely fashion. The Local Government Unit is not responsible for any comments or use of material posted by users.

3.16.2.5 Management of Content with external links

Sharing or re-posting content from other non-Local Government Unit social media accounts is prohibited and are not permitted. For example, links to a personal account/website, individual business account/website or objectionable material as defined in this policy must not be shared or reposted on a Local Government Unit social media account.

It is permissible for the following types of external links

1. Connects the public with information and services provided by the Palestinian government or government-affiliated agencies.
2. Provides further information on subject matter found on the Local Government Unit 's website. Such information must be provided by an official and/or accredited source.
3. A Local Government Unit affiliated organization, service club or registered charity. A professional association or any organization as determined by the Local Government Unit 's Council.
4. Content promoting Local Government Unit events or organized or funded by the Palestinian government or by a service club operating within the Local Government Unit performing work that benefits the residents.
5. Events organized by a registered charitable organization operating within the Local Government Unit.

3.16.2.6 Measuring social media

The social media account administrator will produce a semi-annual report (June, December) on the analysis of the Local Government Unit 's social media accounts to include performance measures for the channel or social media such as: total followers, number of responses, retweets, demographics (Facebook in particular), number of comments, number of complaints, likes and comments.

3.16.2.7 Employees Public Communication

1. No employee or Councilor who is not a Social Media Account Administrator is permitted to post or comment via social media in any way that suggests they are doing it as representatives of the Local Government Unit or in connection with it;

2. An employee or a Councilor may be easily identified as an employee of the Local Government Unit even if they don't explicitly identify themselves as such, so careful consideration should be exercised to ensure that the published information is clearly marked as being the sole owner of the writer and not the Local Government Unit .
3. Any public communications concerning the Local Government Unit must not violate any guidelines set forth in this Policy, any employee handbook or Third Party's contract;
4. Employees and "external parties" may not disclose any sensitive, proprietary, confidential, or financial information about the Local Government Unit. This includes revenues, profits, forecasts, and other financial information, any information related to specific services, customers, or citizens, other than what is publicly available in any of Local Government Unit filings or press releases.
5. Employees and "external parties" may not disclose any sensitive, proprietary, confidential, or financial information about Local Government Unit citizens; including the name of any Local Government Unit citizen and the fact any specific customer has a business relationship with Local Government Unit.
6. Employees and "external parties" may not post any material pertaining to the Local Government Unit, its citizens and/or other external parties that are protected by applicable intellectual property laws (including, but not limited to copyrights and trademarks) unless written permission is obtained from the owner of the intellectual property.
7. Employees and external parties may not attack fellow employees, Third Parties, Citizens and customers, or vendors. Employees and external Parties may respectfully disagree with the Local Government Unit actions, policies, or management.
8. All corporate and separate social media accounts must adhere to Palestinian applicable laws, regulations, and policies, including other applicable Local Government Unit policies.
9. Incidental or occasional personal use of social media on personal or workplace devices is allowed, providing such limited use will not result in any measurable expense to the Local Government Unit in time, material, or productivity, and is subject to the limitations of this policy.

3.16.2.8 Local Government Unit Council social media presence

Accounts belonging to the Local Government Unit Mayor or Councilors must be created and maintained by the owner and not by a Local Government Unit employee unless a decision is made by the Council to that regard. Social Media Account Administrator is permitted to share/re-post content from posts belonging to the Local Government Unit Mayor or Councilor, if the content does not clearly promote or criticize a Palestinian political party, candidate, or ideology. At the beginning of an election year, Social Media Account Administrator will take precautions regarding publishing links, likes and sharing content posted on the Mayor or the Councilor site until the inaugural meeting of the newly elected Council or end of elections. Appropriate sharable

content includes, but is not limited to, community events, funding announcements, bill/law announcements, etc.

3.16.2.9 Password Management & Security

Local Government Unit Corporate and Separate accounts credentials and details must adhere to the **Password Policy** requirements and must be documented and filed in a safe location inside the Local Government Unit with the knowledge of the Local Government Unit General Official and IT department official. If IT department is providing the hosting for the website, access to the website would be granted only to the Social Media Account Administrator. The Local Government Unit's IT Department will maintain a master list of the Local Government Unit 's social media login information. Password changes must be immediately communicated to the IT Department official. Accounts created to represent the Local Government Unit must be associated with a valid Local Government Unit email address: (------@Local Government Unit .ps).

3.16.2.10 Website Disruption

In addition to the guidance mentioned in the **Disaster Recovery Policy**, the following guidance helps Social Media Account Administrator address the possible disruption in the Local Government Unit website and/or social media accounts:

1. Website host to be notified immediately or Local Government Unit IT department Official/ Emergency Committee must be notified immediately (if site is hosted internally) as stipulated in the **Risk Management Policy**.
2. Change passwords.
3. Replace with clean copy of the data

3.16.2.11 Records Management and Retention

Posts/user content deemed to be "Official Records" must be retained and purged according to the Local Government Unit 's **Backup Policy**. Posts/user content that is considered a Transitory Record of the Local Government Unit is not required to be retained and may be purged from social media sites. Any content removed based on the guidelines will be retained by the Social Media Account Administrator, and have supporting documentation, including the time, date, identity of poster, reason for removal, and any required incident reporting.

3.16.2.12 Policy Communication

This policy will be communicated internally with the staff and posted on the Local Government Unit website for public use if needed. All information created on Corporate and Separate social media accounts using Local Government Unit technology is the property of the Local Government Unit. Reasonable technological and procedural measures, including auditing and

random monitoring of social media accounts, will occur to ensure adherence to corporate policies and standards.

3.16.2.13 Related Policies

1. Password change Policy.
2. Disaster Recovery Policy.
3. Risk Management Policy.

4 References

The following references were used as a guidance only:

1. General policy for information security in ministries and government institutions, Ministry of Communications and Information Technology, Palestine, Policies (pna.ps), Palestinian Cabinet Ministry no: (م.و\م.أ\18\112\09)
2. ISO 73/2009
3. ISO/IEC 38500: Internationally accepted as the standard for Corporate Governance of IT
4. NIST: National Institute of Standards and Technology
5. NIST 800-53: Newton, J. (1987), Guide on Data Entity (Naming Conventions), Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online],
6. NIST – www.nist.gov : Ross, R. (2012), Guide for Conducting Risk Assessments, Special Publication (NIST SP), National Institute of Standards and Technology, Gaithersburg, MD, [online], https://doi.org/10.6028/NIST.SP.800-30r1 (Accessed October 20, 2021)
7. NIST password Guidelines and Best Practices for 2020, www.nist.com
8. ISO/IEC 31010:2019 – Risk Management – Risk Assessment Techniques
9. ISO/IEC 27000-018 - Information technology -Security Techniques- Information security management systems- Overview and Vocabulary
10. ISO/IEC 24762:2008 Information technology- security techniques – guidelines for information and communications technology disaster recovery services.
11. ISO 24762 - 5 clauses:

- Clause 5: IT Disaster Recovery.
- Clause 6: IT Disaster Recovery facilities.
- Clause 7: Outsourced service provider's Capability
- Clause 8: Selection of recovery sites
- Clause 9: Continuous improvement

12. ISO 37500:2014: Guidance on Outsourcing
13. ISO 9001: Quality Management Systems - Requirements
14. ISO/IEC 27040:2015 – Information Technology – Security Techniques - Storage Security
15. ISO Guide 73, Risk Management
16. ISO /IEC 27001:2013, Information Technology-Security Techniques-Information Security Management Systems - Requirements
17. ISO /IEC 27002:2013, Information Technology (Security Techniques – code of practice for information technology controls).
18. ISO 27002: Information technology — Security techniques — Information security management systems
19. ISO/IEC 17799: Edition 1, 2000 – Information Technology – Code of practice for Information Security Management

20. ISO 9001: Quality Management
21. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=900402;
22. University of Waterlow Technology abbreviations: /www.allacronyms.com/technology/abbreviations;
23. OECD (2015), Digital Security Risk Management for Economic and Social Prosperity. OECD Recommendation and Companion Document, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264245471-en
24. Control Objectives for Information Technology (COBIT)
25. Information Technology Infrastructure Library (ITIL)
26. Information Technology Infrastructure Library "ITIL", Change management

5 Appendix 1: Fundamentals of an IT system

Fundamentals of an IT system (Minimum Operational Standards)	Explanatory note to answer the lead

1	**Internet Connection** A constant high-speed connection that provides access to email, software updates and other critical services, such as web-based applications.	Yes	No	Not Sure	Local Government Unit must have a constant high-speed connection categorized: **Best**: Fiber connection, **Better:** Cable connection. **Good:** DSL connection
2	**File Backup** All critical data are regularly backed up in some fashion.	Yes	No	Not Sure	is the data backed up, replicated for business continuity and disaster recovery?
3	**Strong Passwords** Passwords are subject to formal rules on format (number of characters, case, numbers and symbols) that apply to Local Government Unit accounts and the passwords are changed regularly, non-duplicated, and protected.	Yes	No	Not Sure	Permission is granted through User Logins, Accounts and Passwords
4	**Anti-Virus (Licensed) on all Computers** Free antivirus (versus paid subscription) options such as AVG or Microsoft Security Essentials not licensed for Commercial or Government use do not meet the requirement of a "Yes" response.	Yes	No	Not Sure	Antivirus/Antimalware product can prevent the infection through installation of protective technologies
5	**Computers running up-to-date (vendor supported) software** Regular, proactive downloading and installation of software updates for the current version (not version upgrade) regularly or are automated for each software application (Operating system, browser, third party software, etc.)	Yes	No	Not Sure	Monthly maintenance (patches, updates, cleaning, etc.) and monitoring plans should be identified for Hardware and Software. Inspection can be used to verify maintenance of updates.

6 Appendix 2: Asset Management

Annual IT Evaluation Checklist: Asset Management					Advisory Notes
1.1	Is there an accurate detailed inventory of hardware?	Yes	☐ No	☐ Not Sure	IT Asset officer to ensure proper Inventory data
1.2	Is there an accurate detailed inventory of software?	Yes	☐	☐	Inventory data collection is the key to proper asset

			No	Not Sure	management
1.3	Is there a scheduled/periodic review of hardware and software to update the inventory?	Yes	☐ No	☐ Not Sure	Maintenance and monitoring are recommended for all hardware and software
1.4	Is there a hardware replacement schedule in place?	Yes	☐ No	☐ Not Sure	Standardization, tracking and usage agreement(s) of the Hardware and Software assets is helpful to build accurate Asset Management.
1.5	Is there a software replacement/upgrade schedule in place? (General - MS Office, departmental level)	Yes	☐ No	☐ Not Sure	Standardization, tracking and usage agreement(s) of the Hardware and Software assets is helpful to build accurate Asset Management
1.6	Is there clear oversight of IT expenditures?	Yes	☐ No	☐ Not Sure	Important to include in the Local Government Unit budgets – three-year plan is suggested
1.7	Is there an established protocol for annual IT expenditures, whether through the operating budget or capital budget?	Yes	☐ No	☐ Not Sure	An essential element to include in any IT plan

7 Appendix 3: Service Request Form model

Local Government Unit Name	**-Service Request Form- Helpdesk Department**	
Employee Name اسم الموظف		
Phone Extension هاتف		
Department Name/Branch الدائرة أو الفرع		
Date Request Reported تاريخ طلب الخدمة		
Brief Description الخدمة المطلوبة بشكل مختصر		
Request Type نوع الخدمة	☐ Service Request طلب خدمة جديدة	☐ Support Request طلب خدمة دعم فني لمشكلة

Department Official Authorization

توقيع مدير الدائرة

_____

8 Appendix 4: System Change Request Form

Local Government Unit Name **System Change Request Form**			
All System Change Requests should be submitted to the Helpdesk (# Business Days) in advance. All System Change Requests must be approved before any changes can be made. Only in an emergency, requests will be expedited			
Requester Name:			
Implementer Name:			
Change Information			
Type Of Change:			
Reason For Change:			
Features/Configuration Changes:			
Impact Of Change:			
Location Of Change:		Systems:	
Number Of Users/Sites Affected:			
Start Date:	Start Time:	End Date:	End Time:
User Notification Required?			
Test Plan:			
Back Out Plan:			
Authorized Official Name:		Signature:	
Authorized Official Name:		Signature:	
Change Control Meeting: Approved ☐		Denied ☐	
If Denied, Provide Reason:			
Post Change Follow-Up			
Date Completed:	Successful ☐	Unsuccessful ☐	Rescheduled ☐
Help Desk Confirmation Date: Helpdesk Request or Reference #		Confirmed By:	

9 Appendix 5: Major Incident Report Form

Local Government Unit Name		**Major Incident Report Form**	
Section I – Description of Incident **All severity one and two reports are due within 24 hours upon closing of the outage.**			
Incident Name:			
Incident Date:	Report Date:		
Helpdesk request / reference Number	Total Resource Hours:	Total Down Time:	
Section II –Incident Details			
Type Of Incident: System Failure ☐ Hardware Failure ☐ Application Failure ☐ Others ☐			
Suspected Cause			
Affected Location	Hq ☐ External office ☐	If External office, Name:	
Affected System(S)		Affected Application	
Type Of System(S)/Data Affected or Damaged			
Severity Of Damage		Backup Or Restore Preformed	
Time Down:	Time Up:	Total Time Down in Minutes:	
Section III Summary			
Reporting Employee:			
Incident Summary:			
Order Of Events:			
Conclusion			
Action Taken			

Recommendations	

10 Appendix 6: Information Security Exemption Form

Local Government Unit Name:
Information Security Exemption Form

Purpose

♦ It Is the Responsibility of each Unit to complete this form when an Information Security Exemption to the Local Government Unit Security Policies or Standards Is Necessary. Please Refer to The Security Policies or Standards.

♦ The Information Security Officer Will Review the Request for Acceptance

Section I: Requester Information

Requester Name			Request Date		
Department Name			Requester Phone No:		
Helpdesk Ticket Number		Begin Date		End Date	

Section II – Exemption Information

This Exemption Applies To	☐ Application Name:_____ ☐ Server Or Device Name:_____ ☐ Others:_____ ☐ Access Level:_____
Purpose	

Affected Location(S)	Main Location ☐ Branch ☐	If Branch, Name of Branch(S)	
Exemption Description			

Exemption Justification:
Exemption Details:
Exemption Summary:

11 Appendix 7: Template Example for Testing backups

Restore Testing Template	**Municipality Name:**
a) Responsible person:	*b) Location / dept.:*
c) Date:	

SERVER BACKUPS TESTED:

1.☐ server OS: .....

2.☐ server OS: .....

3.☐ server OS: .....

4.☐ server OS: .....

5.☐ server OS: .....

DATABASE BACKUPS TESTED:

1.☐ database: .....

2.☐ database: .....

3.☐ database: .....

4.☐ database: .....

5.☐ database: .....

OTHER BACKUPS TESTED:


SOCIAL NETWORK