# Operational Manual Information Technology Department

## INTRODUCTION

The main objective of this Operational Manual of the I.T. Department of Kinyo Virginia Inc., is to establish its internal organization, update its functions, its Human Resources, Policies and Procedures required to meet its objectives.

In the first and second chapters of the Manual, its internal organization, the functions, and requirements of the positions that make it up are described,

Next, in the third chapter, the policies that Kinyo Virginia Inc., (KVI) will implement in terms of systems are detailed, the policies have been analyzed and elaborated, to always comply, in this phase the administrative, technical, and operational work standards are determined, divided into generic and specific, the first determine the internal administrative process and for KVI. The latter determine the technical and operational process.

Chapter IV presents the procedures that the different users must follow in the provision of the services provided by the I.T. Department.

The procedures detail the activities that are carried out, according to the functions of each of the areas that involve this department. Examples of this, the processes to attend a computer equipment service, evaluate a computer equipment, provide preventive and corrective maintenance, register a network account, among others, are described.

The I.T. Department is responsible for ensuring the proper functioning of the data network, systems, computer equipment and that these have an optimal performance; involving users through training courses, consultancies, communications on the Intranet, and informative brochures, which help raise the computer culture.

This Manual has been prepared based on the organizational structure of Kinyo Virginia Inc., (KVI), and the demand and supply of services in systems that the different units that make up this structure require in the management of their processes and procedures.

## OBJECTIVE

Ensure that computer resources are used optimally, providing a quality service that has an impact on the benefit of users. Likewise, to provide a basis through research, analysis, tests and validations to formulate proposals with the intention of continuously improving the technological infrastructure of the information currently used, which allow optimizing the process of providing services in the field of communications, as well as to make known to all the personnel that make up the I.T. department the functions that must be performed, without any objection, publicize the established policies, as well as comply with each of the

procedures in which they intervene. In the same way, to inform the different dependencies of KVI of the service policies and procedures to facilitate and guarantee the proper functioning of the computer resources.

**CHAPTER I**

## DEPARTMENT DESCRIPTION

# 1. DEPARTMENT DESCRIPTION

## 1.1. Objectives of the I.T. Department

The Main Objective of the I.T. Department is to plan, coordinate, execute, train, and supervise the support services in the systems, required by the different Units that make up the internal structure of Kinyo Virginia Inc.

## 1.2. Mission of the I.T. Department

Ensure that the different Units that make up the organizational structure of KVI, receive a timely service in terms of systems taking advantage of and managing these resources efficiently and effectively.

## 1.3. Main Functions Delegated to the I.T. Department

1.3.1 Plan, coordinate, direct and implement the development, and systematization (Software) of the different processes.

1.3.2 Recommend the quantities and technical specifications of the computer equipment (hardware) that is required in the different Units, according to the demand for services that they have or by the implementation of new systems.

1.3.3 Develop and keep updated the communications system (Internet, e-mail, Web Sites, internal networks, external, on-premises system, and cloud) according to the requirements and the integration of processes approved.

1.3.4 Periodically evaluate the security of the Hardware and in terms of:

- Installed capacity, obsolescence, maintenance, physical space, electrical installations, backups, and networks.
- Virus protection.
- Their use in such a way that these resources are managed efficiently, economically, and effectively.

1.3.5 Ensure that all systems (Software), developed in-house and subcontracted through suppliers, have the Technical Program Development Manuals and User Manuals in accordance with the terms of the contract.

1.3.6 Ensure and maintain an updated record on the administration of Software licenses, which are used by different users.

1.3.7 Keep current applied computing technology, or possible applications through advances distributed by providers or over the Internet.

1.3.8 Provide technical support and advice to the different Units in the use of Hardware and Software.

1.3.9 Manage the access codes of the Hardware and Software, authorized to the different users.

1.3.10 Keep updated the inventory of Software that is used and the installed capacity of the Hardware.

1.3.11 Develop and implement a training plan on the use of the Authorized Software.

## 1.4. Internal Structure of the Department

The IT Department of KINYO, is made up of the following positions:

A. I.T. Manager

B. Junior System Analyst

C. Senior System Analyst

## 1.5. Hierarchical Dependency

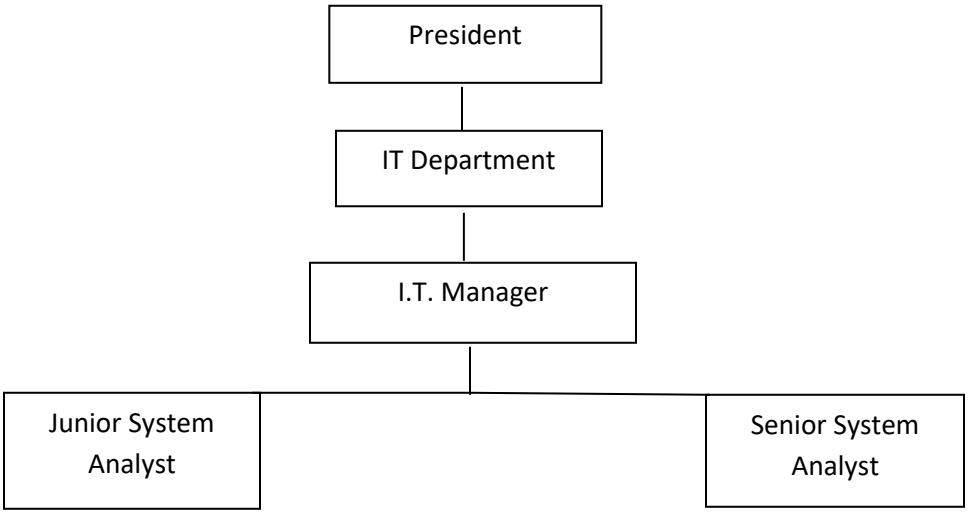
The I.T. Department reports hierarchically to the President.

## 1.6. Internal Organizational Structure

The sheet below shows the internal organizational structure of the I.T. Department.

**I.T. DEPARTMENT**

INTERNAL ORGANIZATIONAL STRUCTURE



**CHAPTER II**

## 2. FUNCTIONS COMMON TO POSTS OF HEADSHIP

All the positions of leadership that coordinate the Units by which their description of functions is included in the Manual of Functions and Requirements of the Position of Kinyo Virginia Inc., have in common a series of duties and responsibilities inherent in the process of administering the work of a group of subordinate persons.

For that reason, they are stated only once, and it must be understood that they are applicable and are part of the duties and responsibilities of the I.T. Department.

### 2.1 Planning Duties and Responsibilities

2.1.1 Carefully plan activities, define objectives, goals, and budgets, which are satisfactorily framed in the total plans of the Department.

2.1.2 Define the duties, responsibilities, and authorities of their subordinates, ensuring that they clearly understand their functions and how to perform them within the limits of their capabilities.

### 2.2 Duties and Responsibilities and Motivation and Coordination.

2.2.1 Seek broad communication and participation of his subordinates in all matters that concern him or may be of interest to him.

2.2.2 Support the development of your staff through their constant evaluation, guidance, and training, to improve them in the performance of their work and create possibilities for progress.

2.2.3 Participate in the preparation and design of crystal reports, Dashboard, Universal Function (Macros, SQL Report, etc.).

2.2.4 Ensure adequate coordination of the work of their subordinates by fostering their trust and spirit of cooperation.

2.2.5 Maintain harmonious working relations between your department and the other Kinyo Virginia Inc., units, and coordinate with them in all that is convenient to ensure the effective progress of the projects, programs, and services of the same.

### 2.3 Duties and Responsibilities of Supervision, Control and Monitoring.

2.3.1 Define indicators, standards, and other bases to evaluate the progress of its department and each of its members, in the fulfillment of the objectives and plans established.

2.3.2 Constantly evaluate the overall effectiveness and efficiency of your department.

2.3.3 Exercise permanent control over the individual performance of their subordinates to:

a) Determine their degree of efficiency in the fulfillment of their duties.

b) Timely correct the failures that are observed and the deviations from the established procedures and systems.

c) Have good evidence for performance appraisal purposes

d) Maintain among their subordinates a high level of discipline and a work environment that promotes maximum productivity.

2.3.4 Ensure the care of the assets assigned to the department and supervise the conditions and use of computer hardware throughout KVI.

### 2.4 Other Duties and Responsibilities

2.4.1 Execute those activities that are not stated in their job description; are within his competence and entrusted by his immediate superior

### 2.5 Functions Common to Non-Chief Positions.

***Non-head positions shall have the following common functions:***

2.5.1 Prepare reports on the functions performed for submission to the Head of the I.T. Department

2.5.2 Attend work meetings, attending invitation or call from the immediate management.

2.5.3 Perform other functions related to the position that are entrusted to him by the immediate President.

**CHAPTER III**

## 3. KINYO VIRGINIA, INC, IN THE I.T. AREA WILL ADOPT THE FOLLOWING POLICIES:

### 3.1 General

3.1.1 All personnel must adhere to the guidelines set out in the Internal Policies of the I.T. Department, regarding the administration and use of computer equipment, data network, manuals, and accessories.

3.1.2 All equipment of information and communications technologies may not be removed from the offices of Kinyo Virginia Inc., for work or personal purposes, except with the prior authorization of the I.T. and the head of the area responsible for the asset.

3.1.3 No computer equipment can be changed without consultation with the I.T. department and in any case, you must request it with prior authorization.

3.1.4 The staff of the I.T. department must deliver a weekly report of their activities via e-mail to the I.T. Department.

### 3.2 Acquisition and Improvements

3.2.1 The acquisitions and improvements of hardware, facilities, software as well as their implementation, will be previously approved by the President.

3.2.2 The technical opinion for the acquisition, lease of goods and / or computer services and communication equipment is considered a confidential document and is for exclusive internal and official use for the I.T. department.

***The equipment requested in the justification project must consider the "Minimum Technical Characteristics", established by the I.T. Department. If, due to the nature of the functions, the Applicant Department requires equipment with superior, special, or specific technical characteristics that are not considered, they must be supported within the justification project.***

3.2.3 The I.T. Department, when planning the operations related to the acquisition of Computer Goods, will establish priorities and in its selection must consider technical study, price, quality, experience, technological development, standards, and capacity.

## 3.3 Hardware and Software Maintenance

3.3.1 The maintenance of the hardware and software will be carried out only by the I.T. Department.

3.3.2 The I.T. Department will only provide the corrective maintenance service to the computer equipment that belongs to KVI.

3.3.3 The I.T. Department would carry out the corrective maintenance of the computer equipment that is no longer under warranty, if the damages caused to it have been due to normal use.

3.3.4 The staff of KVI outside the I.T. Department, are not authorized to uncover the computer equipment.

3.3.5 The I.T. Department will not be responsible for unsupported information of the equipment under repair.

3.3.6 All verified KVI equipment must be labeled with a receipt number, which is used to keep track of each part of the equipment, as well as being registered in the computer system.

## 3.4 Service Orders

3.4.1 All service orders will be handled by the I.T. Support Assistant being assigned a service number (osTicket number) for follow-up.

3.4.2 Any service required by the user must be performed by means of a "Kinyo osTicket Support". These include:

- Repair of equipment failures
- Installing Authorized Software
- Support ERP (Enterprise Resource Planning), Microsoft Office, Teams
- Basic Advice
- Installation of equipment
- Network, Voice, and Data
- Information Systems
- Other.

3.4.3 All computer and communications equipment that enters or requires leaving the I.T. Department or outside the facilities of KVI, for reasons of repair, must be supported by an entry-exit voucher signed by a department manager.

3.4.4 It is the obligation of the outside repair technicians to pass to the I.T. Department, the calendar of preventive maintenance to computer and communication equipment and communicate the dependencies. Outside repair technician will provide information for the preventive maintenance to Servers, network data, and programming by the corresponding personnel.

3.4.5 The technical staff must deliver daily repair reports to the I.T. Manager.

## 3.5 Software Development Platform

All software development that is done in KINYO, will be carried out under the following platform:

3.5.1 Platform: Microsoft SQL (Server) or MySQL, for servers

3.5.2 Network type: Structured star 100 megabyte or higher, wireless

3.5.3 Windows or Linux environment and according to technological advances.

## 3.6 Automation ERP

The execution of the automation and support of the universal function, B1 Dashboard, B1 Validation System, Function Buttons, Mandatory Fields, will be done applying the following:

3.6.1 By I.T. staff, the delivery of source code which must contain the programming tables and relational diagram must be included in the services.

3.6.2 All automation must be validated by users and I.T. staff.

3.6.3 Technical and User Manuals and their updated versions.

## 3.7 Acquisition of Computer Hardware

3.7.1 No rebuilt hardware (even if it is branded) will be purchased.

3.7.2 Any acquisition must be authorized after study by the I.T. Department, in relation to the needs of the user.

3.7.3 The replacement of the hardware will be done as needed, considering the usage and the financial situation of KVI.

3.7.4 All hardware purchased will be branded with preference (HP, Dell, Lenovo, Apple, Microsoft surface, and others) to those with quality reputation.

3.7.5 All Computer Hardware that is purchased must have a warranty.

3.7.6 All equipment purchased must be reviewed by the I.T. department and verify that they meet the corresponding specifications.

3.7.7 The I.T. Department is responsible for carrying out the review of the equipment periodically to keep the equipment belonging to KVI in optimal condition.

3.7.8 The I.T. Department will assign the personnel to carry out a review of the equipment belonging to KVI.

## 3.8 Communications System

As for the communications system, the following aspects must be considered:

3.8.1 The updating and administration of the website will be under the responsibility of the I.T. Department.

3.8.2 All internal and external communications facilities (networks) must be acquired and contracted according to the technical specifications issued by the I.T. department.

3.8.3 Creation, maintenance and updating of user accounts, to access: the internet, mail, internal network, remote access.

## 3.9 Software and Hardware Security

3.9.1 Annually, an operational audit of all the systems that are handled in KVI will be carried out, this will be carried out jointly by the ISO department and the I.T. Department or through 3rd party services.

3.9.2 All computing hardware must have the authorized and updated version of antivirus, or its replacement installed.

3.9.3 Every user will be responsible for the information they manage, for this they must keep a backup copy on the Microsoft OneDrive, SharePoint and in the "Documents" folder, applying the procedures authorized by the I.T. Department.

3.9.4 The I.T. Department will provide weekly and monthly backups of databases, on solid state drive which will be kept in the I.T. Department safe and another copy on the cloud.

3.9.5 All server hardware and network equipment must be protected by electrical protection systems (UPS), insurance against damage and be in offices that have temperature environments ranging between 17 and 22 degrees Celsius. All other computer equipment should be on a surge protector.

3.9.6 The I.T. Department must provide the necessary protection and control mechanisms to ensure the integrity and privacy of the data stored in the files and databases that it has in custody.

## 3.10 Management of Technical and User Manuals

3.10.1 All User Manuals must be provided in electronic form like doc, pdf, files and SharePoint or OneDrive.

3.10.2 Any update of User Manuals must be communicated, installed, and trained by the I.T. Department and ISO department.

3.10.3 All programs owned by KVI must have the sources and technical manuals.

## 3.11 Software Licenses

3.11.1 All licenses for use by KVI will be acquired from authorized distributors, and it will be the direct responsibility of the Executives and Employees for the unauthorized use of such licenses.

3.11.2 The I.T. Department is the only one that may install or uninstall software on computers and the use of unauthorized, or unlicensed software is prohibited., Anyone from the I.T. Department, upon detecting the presence of unauthorized software on Kinyo Virginia Inc., equipment, has the authorization to remove them immediately.

3.11.3 After installing new software or issuing a new computer the I.T. Department will ensure that the user signed a document stating that Kinyo has issued the items and that the user will never attempt to make hardware changes, install software, alter license keys, or introduce unauthorized removable media. The document will also include notice not to violate any copyright law, or any other applicable laws.

## 3.12 Advice and Technical Support (Kinyo osTicket Support)

The advice and technical support provided by the I.T. Department will be given considering the following:

3.12.1 Support will be provided through Kinyo osTicket Support.

3.12.2 The answers will be made of preferences via osTicket.

3.12.3 Requests will be dealt with within a maximum period within the (SLA) service level agreement.

- ☑ SLA1 – 16 business hours
  - ❖ Tier 1, technicians for basic customer issues such as solving usage problems and fulfilling service desk requests that need I.T. involvement.
- ☑ SLA 2 – 24 business hours
  - ❖ Tier 2, engineer experienced, and knowledgeable technician assess issues and provide solutions for problems that cannot be handled by tier 1.
- ☑ SLA 3 – 48 business hours
  - ❖ Tier 3, access to the highest technical resources available for problem resolution or new feature creations. Engineer attempt to duplicate problems and define root causes, using product designs, codes, or specifications. Once a cause is identified, the company decides whether to create a new fix, depending on the cause of the problem. New fixes are documented for use by Tier 1 and Tier 2.

## 3.13 Authorized Access Codes to different Users

3.13.1 The access codes of the users to the programs will be authorized by the head of Division and Department that has the responsibility of said software will be created by the I.T. Department.

3.13.2 The I.T. Department will monthly verify the proper distribution of access to the different programs and will issue the corresponding report to be distributed to the people responsible for the authorization.

## 3.14 Multipurpose Hardware

3.14.1 The I.T. Department will be responsible for exercising custody, planning, control, and maintenance of multipurpose hardware such as: Projectors, Hotspot, Printers, Scanners, iPad, and laptops.

## 3.15 Software Inventory

3.15.1 The I.T. Department will maintain the record and inventory of the software used in KVI, including the improvements and updates that are made to the software (Modules) of processes used by the different units.

## 3.16 Training

3.16.1 Any training on the use of software and others that are not used by the units in the registration of their processes, will be planned and coordinated by the I.T. Department.

## 3.17 Confidentiality

3.17.1 When equipment tests are carried out and it is necessary to modify the network environment, it must be restored to its original state as soon as the tests are finished, in addition if the test equipment remains without a handle even for short periods of time, it must be disconnected or disable its connection to the network.

3.17.2 When link tests are carried out, it must be verified that normal operation is not affected.

3.17.3 It is the responsibility of the Network and Server Administrator that all system files related to the network configuration define access to network services, only to formally authorized users either locally or remotely.

3.17.4 All network services must have connection requirements such as user identification and authentication (name and password).

3.17.5 All unused network services must be deleted, i.e., commands, options, parameters, files, and utilities that are not required.

3.17.6 All files related to the configuration of network services must be assigned access permissions in such a way that they can only be modified by the network administrator or the super-user of the system.

## 3.18 Integrity

3.18.1 All communications equipment will be used only by the staff and with the software authorized by the I.T. Department.

3.18.2 The network administrator is responsible for defining the identification of standards for the definition of addresses used by the computers that make up the institutional network.

3.18.3 The accuracy and integrity of messages flowing on the network must be protected through encryption tools.

3.18.4 It should be ensured that there are no routes to uncontrolled "default" destinations in the routing tables of computers, especially that the tables are not automatically modified with the addition of a "default" path to the system startup time (boot process); likewise, the additions from the routing protocols used must be verified.

3.18.5 Appropriate controls must be established to allow free communication within a group of authorized users, all information sent to another group must pass through a security perimeter.

3.18.6 If the routers do not have the above characteristic, strict controls on the route tables should be maintained, to determine which remote systems can communicate with the local systems.

## 3.19 Availability

3.19.1 All processes associated with network services must be executed automatically at the time of turning on the computer or restarting the operating system, additionally they must notify by means of messages to the operator console and in log files any anomaly or circumstance that prevents its correct operation.

3.19.2 When a network security breach is detected, network services should be disabled until the problem is resolved, the person in charge of the computer center will contact the Network and Server Administrator to indicate the procedure to follow.

## 3.20 Monitoring

3.20.1 The Administrator of Networks and Servers, in coordination with the I.T. Department, shall monitor remote and local networks, support network protocols and use standard management protocols, filter, capture and decode packets of the protocols used, diagnose the state of the network, as well as its performance by analyzing traffic, management of statistics, alarms and alarm thresholds defined by the user.

3.20.2 The necessary monitoring procedures must be established to verify that all processes associated with network services are active and running correctly on the required equipment.

3.20.3 The Network Management system must detect and log security breaches, such as the appearance of unauthorized nodes to the network, duplication or change of addresses assigned to the nodes, network saturation due to a message flow from troubled or network-intensive devices

## 3.21 Access codes (login) and passwords (passwords) for servers

3.21.1 It is mandatory that all servers in the KVI computer network have access codes and passwords.

3.21.2 It is the responsibility of the Network and Server Administrator to keep track of the generated and canceled keys.

3.21.3 The use of the Administrator key and password is the absolute responsibility of the user to whom it has been assigned.

3.21.4 The network administrator and servers, is responsible for the monthly maintenance of the keys and passwords type Administrator of the windows servers and others under its responsibility, understood by this, the revision and debugging of the same, considering the change of functions or positions of the users.

3.21.5 The passwords that are assigned must be at least 14 characters long, with case, numbers, and other characters (those included in the ASCII table).

3.21.6 The network administrator and server are responsible for implementing procedures at the Level of Operating System so that those responsible for each team make the change of passwords automatically with a maximum periodicity of 30 days when required.

## 3.22 Privileged Access Keys for Windows Server Manager

3.22.1 Administrator-type keys or accounts for Windows platform server computers will be considered privileged keys. These items should be renamed when possible.

3.22.2 The I.T. Department is the only area authorized and responsible for the generation, encryption, and control of passwords for the privileged access codes of KVI administrator.

3.22.3 The administrator of networks and servers is responsible for delivering to the I.T. Department, a list of the personnel authorized to receive, when necessary, the passwords of the privileged access keys type administrator, of the equipment under his responsibility.

3.22.4 The personnel authorized to receive privileged keys must have the necessary training and experience, as well as be aware of the responsibilities involved in the reception and, where appropriate, the use of those keys.

3.22.5 Privileged access codes will only be provided to previously authorized personnel and to perform the specific tasks that they have also been authorized to perform according to their functions.

3.22.6 The password for privileged key use provided by the I.T. Department, will be valid according to the time established by the I.T. Department or when its use is no longer needed.

3.22.7 If for reasons of network administration, any technician receives keys from the Administrator, he must strictly follow the actions developed.

3.22.8 Authorized personnel at the time of using privileged access keys, must not develop or use programming of any kind that directly or indirectly affects files, data, or programming in development.

3.22.9 Personnel who use any of the privileged access codes, for no reason should leave a work session open.

3.22.10 In case of emergency, the administrator password will be sealed and kept in the President office.

3.22.11 Only the user with administrator password can change the password of the access keys to the Windows servers.

### 3.23 Corrective or Preventive Maintenance to Servers

3.23.1 The areas responsible for maintenance must notify with due opportunity (at least 2 business days) to the I.T. Department, the preventive maintenance plans, to schedule the use of privileged keys.

3.23.2 During maintenance, the Server Administrator is responsible for supervising the diagnostic procedures carried out by the technical staff.

3.23.3 The server administrator is responsible for the recording of all the diagnostics and logs appropriate for maintenance.

3.23.4 Server maintenance should include: a complete report that includes the following documentation.

a) Service report filled out by the technical staff responsible for maintenance.
b) Log or logs of diagnoses generated by the technical staff.
c) Date and time maintenance services ended.
d) Confirmation that the server is back online.

### 3.24 Backups on Windows Computers

3.24.1 It is the responsibility of the server administrator to perform or verify that the backups of the server and / or workstations that are assigned to it are made.

3.24.2 The Server Administrator oversees the use, protection, and conservation of all the backups that have been generated or that he has in his custody.

Server backups must comply with the following:

| Application | Ordinary Support | Extraordinary Support |
|---|---|---|
| Operating system | In case of configuration modifications | In case of upgrade or installation of new versions |
| Application Software | In case of configuration modifications | In case of upgrade or installation of new versions |
| Information, Institution Data | Daily | In case of a critical update that may affect the databases |

3.24.3 Servers must be backed up periodically on one of the following OneDrive, AWS S3, G, H, and S drive, and must be recorded in a log.

3.24.4 Extraordinary backups should be saved without reusing the same device.

## 3.25 Internet: Rules for the Assignment and Use of Internet Access Accounts Authorization

3.25.1 Requests for internet accounts will be managed through a memorandum sent to the I.T. Department specifying the general data of the applicant and stating the justification for said request.

3.25.1 The assignment of internet accounts may only be made to duly authorized personnel and for strictly labor purposes.

3.25.1 The I.T. Department will control and manage the internet access accounts, delegating this responsibility to the network and server administrator.

3.25.1 If the accounts are required for personnel with levels different from those authorized, they must be requested by the corresponding department manager. This type of request must be accompanied by a justification, which determines the necessary use of an internet account for personnel of those levels.

### 3.25.1 Information Integrity

3.25.1.1 To strengthen the security of information, procedures to be followed for the application, allocation and correct use of the assigned accounts shall be established and disseminated.

### 3.25.2 Identification

3.25.2.1 The assigned accounts will be a unique representation of the identity of each user, to ensure individual responsibility for their actions on the computer systems or tools at their service. It is required to impose a classification of data and applications for the purposes of audit and delimitation of responsibilities.

### 3.25.3 Confidentiality

3.25.3.1 As a level of security, there is the individual and confidential management of the accounts granted, as well as the assignment of personalized passwords by the end user, taking into account that these passwords should not be affectively related to the user, as an example, the name of the pet, the date of birth, should not be used, Anniversary dates, should not be words of easy interpretation or identification, much less that they are in some dictionary.

3.25.3.2 The loan or disclosure of accounts or passwords is strictly prohibited. Assigned accounts must be strictly personal and non-transferable.

3.25.3.3 The termination of personnel is not a valid reason for the transfer or loan of user accounts; therefore, the Human Resources Manager will immediately deliver to the I.T. Department any changes to employment status.

### 3.25.4 Personal Use

3.25.4.1 Users will assume any responsibility for the negligent use of information obtained over the Internet, as well as damages to third parties and copyright infringement.

3.25.4.2 It is forbidden to use any means of Internet connection, other than the computing and communications infrastructure. In those cases, in which these types of connection are indispensable and cannot be provided through the computing and communications infrastructure, the process of installation and contracting of services will be done in coordination with the I.T. Department

3.25.4.3 It is strictly forbidden to use internet accounts, which have not been granted by the I.T. department.

3.25.4.4 Internet communication software will be provided and configured by the I.T Department. Any other communications software must be removed.

3.25.4.5 The inappropriate use of internet accounts, including the use of the internet for personal, obscene, leisure or mockery purposes that degrades the moral and professional quality of the institution and the personnel who work in it, is prohibited.

3.25.4.6 Misuse of the accounts will be attributable absolutely to the owner.

3.25.4.7 The download of any file from the internet is prohibited. If necessary, the request must be made to the I.T. Department so that it does so in a controlled manner so as not to impair the bandwidth or the introduction of malicious software to the institution's network.

3.25.4.8 It is forbidden to add the operation of the network, systems, or programs, whether internal or of other networks. This attack may be punished by judicial process.

## 3.26 EMAIL

### 3.26.1 Utilization

3.26.1.1 The e-mail service must be used exclusively for work purposes.

3.26.1.2 The I.T. Department is responsible for controlling and administering the e-mail service by delegating this responsibility to the network and server administrator.

3.26.1.3 The network and server administrator may propose controls to safeguard the integrity of the email service, as well as the confidentiality of the information that is handled through it.

3.26.1.4 E-mail service will be available to designated employees on and as needed basis determined by management.

3.26.1.5 As a requirement to have email service you must be an active and registered user of the KVI network on a domain account.

3.26.1.6 Only one account will be assigned per user, which will retain the naming characteristics already established for users of the KVI network. I.T. creation, administration and maintenance will be the responsibility of the network and server administrator.

3.26.1.7 Any assigned accounts and usernames are strictly personal, non-transferable and must have an access password.

### 3.26.2 Responsibility of the user

3.26.2.1 The loan or disclosure of accounts, keys, or passwords is strictly prohibited outside of I.T. personnel. Misuse of disclosed accounts will be attributable exclusively to the owner user.

3.26.2.2 Each user key must have a custom access password.

3.26.2.3 The user must store the contents of their mailbox directly on their PC to ensure the preservation of relevant information. This practice is necessary for the freeing up of space on the corporate email server to which each user is validated.

### 3.26.3 Proper Use

3.26.3.1 The email must be used exclusively for work purposes.

3.26.3.2 It is strictly forbidden

a. The use of systems to send mass mail or advertising
b. Send files with description of systems, IP addresses, User Lists, or configuration files.
c. Send usernames and passwords.
d. Submit materials, violating copyright
e. Damage the operation of the network, systems, or programs, whether internal or other networks. This attack may be punished by judicial process.
f. Send messages for commercial purposes except company business purposes.
g. Use inappropriate or obscene language in public or private messages.
h. Send false or damaging messages that may result in economic and intellectual losses.
i. Send messages to external global lists without authorization.
j. Send "chain letters"

k. Send messages of recreation or mockery that degrade the moral and professional quality of the Institution and the staff that works in it.

l. Send messages for the purpose of harassment and / or disrespectful treatment to other users.

m. Introduce malicious software or computer viruses or any other program that corrupts or destroys programs and systems in the institutional network.

3.26.3.3 It is not allowed to delete, browse, copy, or modify messages, folders, files, or data belonging to other users who have not authorized such privileges.

3.26.3.4 Forgery (or attempted spoofing) of e-mail messages is prohibited; as well as reading; deletion; copying or modifying e-mail messages to other users.

3.26.3.5 Information generated or considered the property of the institution, or any other user may not be attached to the messages, unless you have the written authorizations of the functional areas that own said information.

3.26.3.6 For users with access to the internet e-mail service, it is strictly forbidden to use accounts created or acquired from a third-party provider (e.g., Hotmail) from their PC or from any computer in the KVI corporate network.

### 3.26.4 Secure Transmission

3.26.4.1 Any user who accesses, sends, or receives information using the email service, is obliged to the principle of non-repudiation, that is, and will not be able to deny any sending or receiving that is made of their key. It is not exempt in the case of loss, loan, or involuntary disclosure, in any way the use of keys is the absolute responsibility of the user.

3.26.4.2 The messages transmitted and received by the email service are considered records of KVI and may be used for purposes that this institution agrees, including use as evidence for a judicial investigation.

3.26.4.3 Any information attached to e-mail messages that is classified as "confidential" or “restricted use" shall be encrypted before being transmitted to any external e-mail address.

3.26.4.4 All files that are transmitted through e-mail messages should be checked through the antivirus tools available by the I.T. Department and handled with caution to ensure that they do not contain any type of computer virus.

## 3.27 PROPER USE OF PERSONAL COMPUTERS

It is the obligation of every user to turn off the computer equipment at the end of their working day. You must verify that the computer equipment is completely turned off (C.P.U, monitor, regulator)

a) Only the I.T. Department may install or uninstall software on each personal computer.

b) Every computer must be attached to a domain as an indispensable requirement for network services.

c) Every computer must have a password-protected screensaver within 10 minutes of not using it.

d) The system should crash when attempts are made more than three times to enter an incorrect password.

e) The user must not possess administrator privileges on his personal computer.

f) No user should share folders on their personal computer on the network.

g) Removable media must comply with the removable media policy.

h) All personal computers must have a corporate antivirus and it must always be updated.

## 3.28 WIRELESS NETWORK

### 3.28.1 General

Any person with permission to access the Kinyo Virginia Inc., wireless network must follow the guidelines defined in these regulations.

### 3.28.2 I.T. Department

3.28.2.1 The I.T. Department shall establish controls for navigation over the wireless network.

3.28.2.2 The wireless network access point must be configured with WPA2 or higher encryption, either with a pre-shared key or using validation using a RADIUS server.

3.28.2.3 Only the I.T. Department may grant browsing rights over the wireless network to users.

3.28.2.4 Any computer that connects to KVI wireless network must have an antivirus installed and keep it updated.

3.28.2.5 There must be a formal procedure for granting browsing permissions through the KVI wireless network.

3.28.2.6 The I.T. Department shall monitor the use of the wireless network and report as requested to the President.

3.28.2.7 Periodically, penetration tests must be carried out on KVI wireless network, with the aim of verifying compliance with this policy and in the case of finding a vulnerability, it will be notified for immediate solution.

### 3.28.3 Users in General

3.28.3.1 Browsing using the Kinyo Virginia Inc., wireless network is not allowed, without the respective authorization.

3.28.3.2 Navigation will be allowed only to sites related to KVI, and / or that collaborate for the performance of the functions of the work role of each user.

3.28.3.3 Downloads of any kind from the internet are not allowed without the authorization and knowledge of the I.T. Department.

3.28.3.4 Only users who have been authorized by the Network Administrator may make use of instant messaging programs such as: Teams and others.

3.28.3.5 Never use the "Remember password" option for sites that offer this option.

3.28.3.6 When an employee is provided access to the wireless network, they should read this document or have their Network and Server Administrator train them on the proper use of the network.

3.28.3.7 The following is a summary of things that should not be done:

a) Access the wireless network without authorization.

b) Visit pages with content outside their functions within the institution, including pornography, nudism, leisure, etc.

c) Disclose sensitive information of Kinyo Virginia Inc., through the internet and / or through instant messaging.

d) Download from the internet.

e) Use instant messaging programs without authorization.

## 3.29 SEPARATE ENVIRONMENTS

3.29.1 All employees with programming activities must be in a development environment, under no circumstances should they work in Production or access the real data of the institution.

## 3.30 SANCTIONS

3.30.1 Any employee found to have violated this policy may be subject to disciplinary action, which is defined in Schedule 1 Penalties for Non-Compliance with KVI I.T. Policy.

3.30.2 Human Resources must execute the development, training, maintenance, and execution of disciplinary actions of the internal regulations in relation to violations of these regulations.

**CHAPTER IV**

## PROCEDURE ON SYSTEMS SERVICES

## TABLE OF CONTENTS