REPUBLIC OF RWANDA

WESTERN PROVINCE

RUBAVU DISTRICT

P.O. Box: 1 32 Gisenyi

WEB SITE: www.rubavu.gov.rw

E-mail : rubavudistrict@rubavu.gov.rw

ICT ACCEPTABLE USE POLICY

LIST OF ABREVIATION

CD: Compact Disk

DHCP: Dynamic Host Control Protocol

DNS: Domaine Name Service

E-Mail: Electronic mail

FTP: File Transfer Protocol

GB: Giga Byte

GSE: Government Secure Extranet

GSI: Government Secure Intranet

ICT: Information communication technology

IT: Information Technology

ITGC: Information Technology general Control

LASE: List of Approved Software and Equipment

NPS: National Probation Service

NT: New Technology

PC: Personal Computer

SNMP: Simple Networl Management Protocol

TCP/IP: Transimission control Protocol/Internet Protocol

VPN: Virtual Private Network

WWW: World Wide Web

I.IT POLICIES AND PROCEDURES

I.a. INTRODUCTION

Information and Communication Technology (ICT) and the Internet are widely available to staff in RUBAVU DISTRICT OFFICES. The District's technology services offer vast, diverse and unique resources to users providing access to:

- ❖ Computers to process data, save data, speed up, and facilitate service delivery
- ❖ Information and Communication Networks: providing shared network resources and Applications.
- ❖ Internet Access: providing global information and social networking
- ❖ E-Mail: providing opportunities for electronic interpersonal communication
- ❖ Emerging applications to be adopted as appropriate.

The District policies, regulations establish rules for behavior and communication applicable to the use of ICT networks and the Internet. Individuals are responsible for their actions while using the ICT and the Internet. The use of such technology is a privilege not a right. Inappropriate use may result in restrictions or cancellation of access rights and/or further disciplinary action

The ICT service at RUBAVU District's intentions for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to RUBAVU's established culture of openness, trust and integrity. The ICT service at RUBAVU is committed to giving access to RUBAVU's employees, partners and RUBAVU from illegal or damaging actions by individuals, either knowingly or unknowingly.

I.b POLICY STATEMENT

"It shall be the responsibility of the I.T. Department to provide adequate protection and confidentiality of all corporate data and IT tools and accessories such as Computer desktops and laptops, held at RUBAVU District, to ensure that these devices are well maintained. Information and Communication Technology (ICT) is provided to support District activities.

Computers and other ICT facilities may face security breaches that can compromise confidential information and expose the District to losses and other legal risks".

I.c REASON OF ICT POLICY

Accordingly to the internal organization of District, the ICT Policy serves as an acceptable use of technology resource policy , of RUBAVU District

I.d AREA OF EXECUTION

The set is established in RUBAVU District, Western Province only.

I.e DURATION

These internal rules are constituted for unspecified duration.

I.f AMEND

This policy is maintained by the ICT Departement. Requests to change the policy should be made to the Mayor. All changes will need to be approved by District Council.

I.1 EMAIL AND COMMUNICATIONS ACTIVITIES POLICY

The following activities are strictly prohibited, with no exceptions:

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within District's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by District or connected via district's network.

Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

I.2 VIRUS AND MALICIOUS SOFTWARE POLICY

I.2.1 SCOPE OF THIS POLICY

This policy applies to all authorised users of the RUBAVU District environment and is therefore applicable to all staff, whether permanent or temporary, and to any third party contractors or partners who have access to Home Office IT assets and/or the RUBAVU District environment including remote working locations.

I.2.2 VIRUS AND MALICIOUS SOFTWARE POLICY OBJECTIVES

The objectives of this policy are to provide a clear structure for preventing and handling incidents concerning computer viruses and/or malicious software or code by ensuring that:

- All IT assets are protected from both viruses and malicious software or code infection by using NPS approved antivirus software;
- The NPS complies at all times with all minimum technical security requirements according to the current recommended architectures for GSI and GSE Connections;
- All viruses and malicious software or code patterns/signatures are updated on a regular basis according to the prime contractor RUBAVU District contract and local procedures;
- Access to mobile code is controlled within the configuration of the authorised user‟s browser and by the RUBAVU District environment gateway;
- All NPS information transferred electronically into the RUBAVU District environment is scanned for viruses and malicious software or code infection prior to allowing the transfer of the NPS information and therefore prior to execution or use;
- All NPS information processed or modified on any IT asset is scanned at the point of entry to the RUBAVU District environment;

- All incidents where viruses and malicious software or code are detected are treated as a security incident and are reported in accordance with the NPS Incident Management Policy;

- In the event of suspect data of any form having been identified on a authorised user"s system, the authorised user does not under any circumstances review or open such data;

- In the event of a virus or malicious software or code being detected the relevant IT asset is quarantined (i.e. disconnected from the RUBAVU District environment or any other network) and the Local System Controller takes the appropriate actions according to the NPS Incident Management Policy as well as any local procedures;

- No software or equipment is used on the RUBAVU District environment unless it is specifically mentioned on the LASE (List of Approved Software and Equipment) which is kept up to date by the prime contractor;

- Local area procedures and codes of practice, in support of this policy include statements regarding antivirus software management, whom to contact if a computer virus or malicious software or code is suspected, procedures for detecting and managing viruses and malicious software or code and how to check that antivirus software, on all IT assets, are both active and up to date;

- Anyone accessing or using any aspect of the RUBAVU District environment complies with this policy.

I.2.3 ANTIVIRUS

To establish requirements which must be met by all computers connected to the district networks to ensure effective virus detection and prevention.

This policy applies to all district computers that are PC-based or utilize PC-file directory sharing. This includes, but is not limited to, desktop computers, laptop computers, file/ftp/tftp/proxy servers, and any PC based lab equipment such as traffic generators.

All district computers must have district's standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. Virus-infected computers must be removed from the network until they are verified as virus-free. Lab Admins/Lab Managers are responsible for creating procedures that ensure anti-virus software is run at regular intervals, and computers are verified as virus-free. Any activities with the intention to create and/or distribute malicious programs into district's networks (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.) are prohibited, in accordance with the Acceptable Use Policy.

Recommended processes to prevent virus problems:

- Always run the corporate standard, supported anti-virus software is available from the corporate download site. Download and run the current version; download and install anti-virus software updates as they become available.
- Never open any files or macros attached to an email from an unknown, suspicious or Untrustworthy source. Delete these attachments immediately, then "double delete" them by Emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in with district's Acceptable Use Policy.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is absolutely a business requirement to do so.
- Always scan a floppy diskette, CD, Flash Drives,… from an unknown source for viruses before using it.

- Back-up critical data and system configurations on a regular basis and store the data in a safe place.

- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, and then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

- New viruses are discovered almost every day. Periodically check this Anti-Virus Policy for updates.

Noted exceptions: Machines with operating systems other than those based on Microsoft products are exempted at the current time.

I.3 PROGRAM CHANGE CONTROLS

I.3.1 DEFINITIONS

IT General Controls (ITGC) represent the foundation of the IT control structure. They help ensure the reliability of data generated by IT systems and support the assertion that systems operate as intended and that output is reliable. ITGC usually include the following types of controls:

- **Control environment**: or those controls designed to shape the corporate culture or "tone at the top."
- **Change management**: procedures - controls designed to ensure changes meet business requirements and are authorized.
- **Source code/document version control** : procedures - controls designed to protect the integrity of program code
- **Software development life cycle**: standards - controls designed to ensure IT projects are effectively managed.
- **Logical access policies**: standards and processes - controls designed to manage access based on business need.

- **Incident management:** policies and procedures - controls designed to address operational processing errors.
- **Problem management:** policies and procedures - controls designed to identify and address the root cause of incidents.
- **Technical support**: policies and procedures - policies to help users perform more efficiently and report problems.
- **Hardware/software**: configuration, installation, testing, management standards, policies and procedures.
- **Disaster recovery/backup and recovery**: procedures, to enable continued processing despite adverse conditions.
- **Physical security:** controls to ensure the physical security of information technology from individuals and from environmental risks.

I.3.2 CHANGE MANAGEMENT

This chapter provides procedures that will be observed when initiating request for changes to district IT systems. It covers all the IS systems with particular emphasis on the systems currently in use.Change requests will originate from the following areas within the organization:

- **System Users**: as the main group who utilize the systems in place, the users are the best source of change requests. As they use the system daily, they will come with suggestions and complaints about the current system. These will be passed to the ICT service for implementation.
- **The Management**: when policies change within district management, this may indirectly require changes into the current System functionality.

Guideline	Description and Applicable procedures
User Initiated Requests	• The user initiating the request for the change will fill out a Change Requisition Form. • The Change Requisition Form will be passed to his/her supervisor for confirmation and signature. • This will then be handed to ICT Service, which will pursue with the necessary Companies for the implementation of the change into the System. • After receiving the requested change, the ICT Service will test it thoroughly on a test environment in co-ordination with the user. • After satisfactorily testing the solution, the ICT Service will deploy the change into the live environment. • The user will sign the Change Completion Form and this will be filed for future reference.
Management Initiated Requests	• After a meeting with the Management, the ICT Service will fill out the Change Requisition Form. • This form will be signed by the Senior Management after confirmation of accuracy of the request • The ICT Service will pursue with the necessary Companies for the implementation of the change into the System. • After receiving the requested change, the ICT Service will test it thoroughly on a test environment. • After satisfactorily testing the solution, the ICT Service will deploy the change into the live environment. • The ICT Service will fill out Change Completion Form and have it signed by Senior Management. This will then be filed for future reference.

Change Priority	All change requests will be prioritized according to urgency. The following indicators will be used for prioritization: • **Priority 1**: Highest priority. ICT Service should deliver the change within one week of receiving the signed request form • **Priority 2**: Middle level priority. Change has to be implemented within two to three weeks on receiving the signed request form. • **Priority 3**: Lowest Level priority. Change should be delivered within a month of receiving the signed request form.

I.4 ACCESS CONTROL

Access to protect information must be restricted to people who are authorized to access the information. The computer programs, and in many cases the computers that process the information, must also be authorized. This requires that mechanisms be in place to control the access to protected information. The sophistication of the access control mechanisms should be in parity with the value of the information being protected – the more sensitive or valuable the information the stronger the control mechanisms need to be. The foundation on which access control mechanisms are built start with identification and authentication.

I.4. 1 LOGICAL ACCESS CONTROL AND USER

This chapter provides procedures and practices that will be observed during any System User related activities. This policy covers the following exercises:

- User creation, modification and deletion.
- User access privileges creation and modification

Guideline	Description and Applicable procedures
User creation, modification and deletion	• New user creation will be done by the ICT Service at district after receiving a completed and signed 'New User Creation Request' form. • Both the Departmental Head and Human Resources Manager should sign the request form. • A modification Request Form should be duly completed and signed for the ICT Service at district to effect any changes in the already existing users. The Departmental Head, before implementation, must approve this request. • User deletion shall be carried out after the ICT Service at district receives a 'User Deletion Request' Form. The Departmental Head and Human Resources Manager must approve this form.
User access privileges creation and modification	• Access Control Form will be provided to all Departmental heads, which they are to fill indicating all the access and procedure rights each user in his/her department is to be granted. No access rights will be granted to any user without a completed and signed form. • Any modifications to access rights have to be initiated by the user through his/her Departmental Head. A request form has to be completed clearly indicating the reasons behind the access rights change.

I.5 THIRD PARTY

The RUBAVU District will make Contract with contractor in ICT field who will perform the maintainemce of ICT equipments such as photocopy, Printers, televisions, Generator, air conditions, Computers (Laptop and Desktop)

I.6 INFORMATION SECURITY RESPONSIBILITIES

I.6.1 PURPOSE

The purpose of this document is to clearly define roles and responsibilities that are essential to the implementation of the RUBAVU District's Information Security Policy.

I.6.2 SCOPE

These Roles and Responsibilities apply to all staff and third-party Agents of the RUBAVU District as well as any other RUBAVU District affiliate who is authorized to access Institutional Data.

I.6.3 MAINTENANCE

These Roles and Responsibilities will be reviewed by the RUBAVU District‟s Information Security Office every 5 years or as deemed appropriate based on changes in technology or regulatory requirements.

I.6.3 ROLES AND RESPONSIBILITIES

The RUBAVU District's Information Security Policy states that, "Individuals who are Authorized to access The IT best practice through the IT governance and its mechanism recommends that an institution whose activities are significantly IT based should are defined as follows:

- **Executive Strategic Committee**

a. Reviewing and recommending Strategies To promote investment in IT
b. Analyzing the District Planning Strategies impact of proposed strategies on the RUBAVU District environment.
c. Overseeing major projects and managing IT priorities, IT costs and IT resource allocation

- **Executive Steering Committee**

a. Reviewing and recommending strategies to implement the Information Security Policy.
b. Approving proposed strategies.
c. Serving as a champion for accepted strategies within respective District Planning units and/or colleges.
d. Overseeing the review and approval of Information Security Policy exceptions.

- **Director of Human Resources and Administration**

The Director of Human Resourses and Administration is a senior-level employee of the RUBAVU District who oversees the RUBAVU District's information security program. Responsibilities of the Director of Human Resources and Administration include the following:

a. Developing and implementing a District-wide information security program.
b. Documenting and disseminating information security policies and procedures.
c. Coordinating the development and implementation of a District-wide information security training and awareness program.
d. Coordinating a response to actual or suspected breaches in the confidentiality, integrity or availability of Institutional Data.

- **Users**

For the purpose of information security, a User is any employee, contractor or third-party Agent of the RUBAVU District who is authorized to access District Information Systems and/or Institutional Data. A User is responsible for the following:

a. **Adhering to policies, guidelines and procedures pertaining to the protection of Institutional Data.**

Information Security Office publishes the information security various policies, guidelines and procedures related to the protection of Institutional Data and Information Systems. They can be found on the Information Security Office website may also publish their own unique guidelines and procedures. Information on requirements unique to your system you have access to can be found by talking to your manager or system administrator.

b. **Reporting actual or suspected vulnerabilities in the confidentiality, integrity or availability of Institutional Data to a manager or the ICT Deparetement.**

During the course of day-to-day operations, if a User comes across a situation where he or she feels the security of Institutional Data might be at risk, it should be reported to the ICT Office. For example, if a User comes across sensitive information on a website that he or she feels shouldn"t be accessible, that situation should be reported to the Information Security Office. Additional notifications may be appropriate based on procedures unique to a business unit or defined by a Data Steward. It may be appropriate to notify a local security point of contact that will in turn coordinate with the ICT Office.

c. **Reporting actual or suspected breaches in the confidentiality, integrity or availability of Institutional Data to the ICT Office.**

Reporting a security breach goes hand in hand with reporting vulnerabilities. See the Procedure for Responding to a Compromised Computer for more information on what constitutes a security breach and for what steps to take if you suspect a security breach. Once again, it may be appropriate to notify a local security point of contact that will in turn coordinate with the Information Security Office.

I.7 INFORMATION SENSITIVITY CLASSIFICATION

I.7.1 DEFINITION

Information sensitivity: is the control of access to information or knowledge that might result in loss of an advantage or level of security if disclosed to others.

Loss, misuse, modification, or unauthorized access to sensitive information can adversely affect the privacy or welfare of an individual, trade secrets of a business or even thesecurity, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information.

I.7.2 OBJECTIVE

To classify information as to "sensitivity," in order to assure appropriate security measures throughout the lifecycle of RUBAVU District information and information processing facilities.

I.7.3 APPLICABILITY

Information sensitivity classification should occur for all significant information collections of the RUBAVU District , and for the information processing facilities used to access, store or transmit that information.

I.7.4 SENSITIVITY CRITERIA

Sensitivity classification should be based on confidentiality, integrity and availability dimensions of the data relevant to all stakeholders. This could include consideration of:

I.8 PASSWORD MANAGEMENT

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of district's entire corporate network. As such, all district employees (including contractors and vendors with access to district systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any district facility, has access to the district network, or stores any non-public district information.

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the ICT Service administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days. The recommended change interval is every four months.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

Guideline	Description and Applicable procedures
General Password Construction Guidelines	Passwords are used for various purposes at district. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Given that very few systems have support for one-time tokens (i.e. dynamic passwords which are only used once), everyone should be aware of how to select strong passwords. **Poor, weak passwords have the following characteristics**: • The password contains less than fifteen characters

	• The password is a word found in a dictionary (English or foreign)
	• The password is a common usage word such as:
	  • Names of family, pets, friends, co-workers, fantasy characters, etc.
	  • Computer terms and names, commands, sites, companies, hardware, software.
	  • The words "Rubavu", "commission" or any derivation.
	  • Birthdays and other personal information such as addresses and phone numbers.
	  • Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
	  • Any of the above spelled backwards.
	  • Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
	
	Strong passwords have the following characteristics:
	
	• Contain both upper and lower case characters (e.g., a-z, A-Z)
	• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
	• Are at least fifteen alphanumeric characters long and is a passphrase (Ohmy1stubbedmyt0e).
	• Are not words in any language, slang, dialect, jargon, etc.
	• Are not based on personal information, names of family, etc.
	• Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

Password	• Do not use the same password for district accounts as for other non-

Protection Standards	district access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various district access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account. • Do not share district passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidentialdistrictinformation. Here is a list of "dont's": • Don't reveal a password over the phone to ANYONE • Don't reveal a password in an email message • Don't reveal a password to the boss • Don't talk about a password in front of others • Don't hint at the format of a password (e.g., "my family name") • Don't reveal a password on questionnaires or security forms • Don't share a password with family members • Don't reveal a password to co-workers while on vacation • If someone demands a password, refer them to this document or have them call someone in the ICT Service. • Do not use the "Remember Password" feature of applications (e.g., Outlook, Netscape, Messenger, Internet Explorer, Firefox…). • Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. • Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change

	interval is every four months. • If an account or password is suspected to have been compromised, report the incident to The ICT Service and change all passwords. • Password cracking or guessing may be performed on a periodic or random basis by The ICT Service or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.
Application Development Standards	Application developers must ensure their programs contain the following security precautions. Applications: • Support authentication of individual users, not groups. • Should not store passwords in clear text or in any easily reversible form. • Provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password. • Support security retrieval, wherever possible.
Use of Passwordsand Passphrases for Remote Access Users	Access to the district Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.
Passphrases	• Passphrases are generally used for public/private key authentication. 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. • Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

	• A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase: • "The*?#>*@TrafficOnThe101Was*&#!#ThisMorning" • All of the rules above that apply to passwords apply to passphrases.

I.9 USE OF INTERNET

Define policies and procedures for access to the Internet throughout the District network infrastructure.

This policy applies to all personnel with access to Internet and related services through the District network infrastructure. Internet Related services include all services provided with the TCP/IP protocol, including but not limited to Electronic Mail (e-mail), File Transfer Protocol (FTP), Gopher, and World Wide Web (WWW) access.

Access to the Internet through the District is a privilege. Users granted this privilege must adhere to District guidelines concerning the appropriate use of this information resource. Users who violate the provisions outlined in this document are subject to disciplinary action up to and including termination. In addition, any inappropriate use that involves a criminal offense will result in legal action. All users are required to acknowledge receipt and understanding of guidelines contained in this document.

Guideline	Description and Applicable procedures
Acceptable Use	• Access to the Internet is specifically limited to activities in direct support of official District business. • In addition to access in support of specific work related duties, the D • District Internet connection may be used for educational and research purposes.

	• If any user has a question of what constitutes acceptable use he/she should check with their supervisor for additional guidance. Management or supervisory personnel shall consult with the Information Systems Director for clarification of these guidelines
Inappropriate Use	• The District, Internet access shall not be used for any illegal or unlawful purposes. Examples of this would be the transmission of violent, threatening, defrauding, pornographic, obscene or otherwise illegal or unlawful materials • The District, Internet access shall not be used for private, recreational or other non-District related activity. • The District Internet connection shall not be used for commercial or political purposes. • Use of the District, Internet access shall not be used for personal gain such as selling access of a District user login. Internet access shall not be used for or by performing work for profit with District resources in a manner not authorized by The District. • Users shall not attempt to circumvent or subvert security measures on the District's network resources or any other system connected to or accessible through the Internet. • District users shall not use Internet access for interception of network traffic for any purpose unless engaged in authorized network administration. • District users shall not make or use illegal copies of copyrighted material, store such copies on District equipment, or transmit these copies over the District network.
Security	• District users who identify or perceive an actual or suspected security problem shall immediately contact the District ICT Officer. • Users shall not reveal account password or allow another person to use their account. Similarly, users shall not use the account of another user. • Access to District network resources shall be revoked for any user

	identified as a security risk or a demonstrated history of security problems
Penalties	Any user violating these policies or applicable state, or federal laws is subject to the loss of network privileges and any other District disciplinary actions deemed appropriate.
User Compliance	All terms and conditions as stated in this document are applicable to all users of the network and the Internet connection. These reflect an agreement of all parties and should be governed and interpreted in accordance with the laws of Rwanda.

I.10 MOBILE COMPUTING

I.10.1 OVERVIEW

This document describes the security guidelines that the District has developed for mobile devices (such as Blackberry devices, PDAs, and laptop computers) must be appropriately secured to prevent sensitive data from being lost or compromised, reduce the risk of spreading viruses, and mitigate other forms of abuse of District computing infrastructure.

This guideline applies to all District affiliates. This includes staff members as well as guest account holders.

I.10.2 PURPOSE OF THE GUIDELINE

The District Computing Policy establishes a general policy for the use of computing, telephone and information resources. The purpose of this guideline is to establish acceptable practices that support the policy as it applies to mobile devices.

This guideline was established to ensure that the District community has a clear understanding of proper procedure and usage. Computing Services reserves the right to modify this guideline as necessary. Any changes to this guideline will be posted to official.computing-news and will be reflected on this web page.

I.10.3 GUIDELINE STATEMENT

In order to secure information stored in a mobile device, the District community should adhere to some general "best practices" when using mobile devices. Additional measures may be possible and appropriate for securing your specific device.

I.10.4 USER RESPONSIBILITIES AND PROCEDURES

Password-protect your mobile device: Physical security is a major concern for mobile devices, which tend to be small and easily lost or misplaced. If your mobile device is lost or stolen, a device password may be all that stands in the way of someone reading your email and other sensitive data.

- Choose a strong password. The security of your system is only as strong as the password you select to protect it. **See point I.8**
- It may be difficult to type especially complex passwords on the small keypad of some devices, but it is important that you try to choose a strong, effective password that is not easily guessed. **See point I.8**.

Use antivirus software: Mobile devices can be just as susceptible to viruses as desktop computers. This is new terrain for hackers but, industry analysts expect viruses, Trojans, spam, and all manner of scams to grow as the mobile device market grows. A couple of examples encountered to date include the 911 virus which caused 13 million i-mode users to automatically place a call to Japan‟s emergency phone number and the PalmOS/LibertyCrack, a known Trojan horse that can delete all applications on a Palm PDA.

A number of vendors offer antivirus and anti-spam solutions. Airscanner, F-Secure, and Trend Mobile are a few examples.

Promptly report a lost or stolen device: In some cases, as in the case of District‟s BlackBerry service, a device can be remotely deactivated thus preventing email or other sensitive data from being exposed. Understand what options are available to you and exercise them promptly when necessary. Additionally, consider documenting the serial number of and/or engraving your device.

Verify encryption mechanisms: Your accounts and passwords should never travel unencrypted over a wireless network. Wireless network traffic can be easily sniffed. Therefore, any sensitive

data, especially login information, should always be encrypted. District‟s VPN service provides encryption for some device types.

Sensitive documents, if stored on the device, should be encrypted if possible (keeping in mind that some devices encrypt stored documents by default).

Disable options and applications that you don't use: Reduce security risk by limiting your device to only necessary applications and services. You won't need to manage security updates for applications you don't use and you may even conserve device resources like battery life. Bluetooth and IR are two examples of services that can open your device to unwelcome access if improperly configured.

Regularly back up data: Be sure to have a back up copy of any necessary data in case your mobile device is lost or damaged. Consider using multiple backup mechanisms and if you travel, have a portable backup device that you can take with you.

Follow-up safe disposal practices: When you are ready to dispose of your device, be sure to remove all sensitive information first. Some services, like Computing Services' BlackBerry service, can help by remotely clearing the device.

Other Precautions: Keep power to your device. If it loses power, all stored information may be erased.

II. ROLES AND RESPONSIBILITIES

Just as everyone in the District community is expected to use physical resources at District responsibly, we are all expected to help protect information resources at District. Protecting information resources is not the sole responsibility of IT administrators.

II.1 IT STRATEGIC COMMITTEE

The IT Strategy committee operates at the board level, it seeks to advise the board and management on the IT strategy of the District, it also focuses on current and future strategic IT issues.

The IT strategic committee has the broader role of ensuring there is alignment between IT and business strategy through District IT governance.

Roles and responsibility of the IT Strategic Committee includes :
the Strategy Committee The Strategy Committee is responsible to the Board of Directors ("Board") for the oversight of the Company's Strategic Plan ("Plan").The Committee will maintain an on-going, cooperative, interactive strategic planning process with the Company's executive management, including the identification, setting and maintenance of strategic goals and expectations as well as the review of potential acquisitions, joint ventures, and strategic alliances. References to Company strategy and strategic planning are intended to focus on the Company's medium and long term initiatives versus day to day operations.

Roles and responsibility of the IT Strategic Committee includes:

II.1.2 DELEGATION OF AUTHORITY

The Committee shall have the resources and authority appropriate to discharge its responsibilities, including the authority to retain counsel and other experts or consultants.

II.1.3 MEETINGS

The Committee shall meet not less than 3 times per year and additional meetings may be convened as circumstances warrant.

II.1.4 COMMITTEE DUTIES AND RESPONSIBILITY

The Committee will provide guidance, input and suggestions to the District Council and to the Executive Committee with respect to the District's strategy for the medium and long term. Executive Committee shall devise and develop the District's Plan, and once approved by the District Council, will implement the District's Plan in the day to day operations of the business. The Committee will review the Plan and make recommendations to management on behalf of the District Council as part of its oversight responsibility. Furthermore, the Committee, where appropriate, will also advise and make recommendations to the District Council and Executive Committee about the following:

- oversight of the strategic direction of the District
- development, adoption and modification of the District 's Plan
- responses to external developments and factors, such as changes in the display industry, economy, competition, and technology, which impact the District 's strategy
- acquisitions, joint ventures and strategic alliances
- the development of plans to implement the District strategy

- the review of the District 's progress with respect to implementation of its strategy The Committee will regularly review, discuss, and, where appropriate, make recommendations to Executive Committee on the District 's vision as well as share with Executive Committee the District Council 's expectations for the strategic planning process.
- Reviewing and approving of major IT projects;
- Provide IT insights to board and act as subject matter expert
- Promoting two way communication between business and IT;
- Monitor strategic IT plans
- Enhancing the understanding and satisfaction of the value of an IT investment;
- Understand, communicate, Mitigate IT risk

II.1.5 MEMBERSHIP

The Committee is composed by:

- President of Joint Action for Development Forum (JADF)
- Secretary of District Council
- Network and System Administrator
- Director of Planning
- Logistics officer

The President of Joint Action for Development Forum (JADF) will heading the Committee whereas the Network and System Administrator will act as Secretaryof the committee.

II.2 IT STEERING COMMITTEE

An IT steering committee is a key component in IT governance since it provides the strategic alignment required to fulfil the District" goals and objectives. Top management usually establishes the committee to oversee the information systems function and activities. It is a mechanism that ensures the IT section is in harmony with the corporate mission and goals.

Some of the basic roles and responsibilities performed by the IT Steering committee includes:

- Ensuring the alignment of the IT strategy with the District"s strategy;
- Enhancing the understanding and satisfaction of the value of an IT investment;

- Promoting two way communication between business and IT;
- Reviewing and approving of major acquisitions;
- Reviewing and approving of major IT projects;
- Reviewing and approving of plans to outsource IT activities;
- Reviewing the adequacy and allocation of resources;
- Making decisions with regard to centralisation and decentralisation;
- Supporting development and implementation of an organisation wide information security management program; and

Reporting to the Executive Committee on IT activities

II.2.1 DELEGATION OF AUTHORITY

The ICT Steering Committee must be established by the RUBAVU District Executive Committee and approved by District Council. It is a permanent committee with recommending powers.

II.2.2 MANDATE

1. Develop and sustain the ICT plan for the District and approval District Executive Committee In order to accomplish its activities ICT Steering Committee will:
    a. Collect ICT related information from any activity area of the District as required; b. Coordinate the ICT components of the ICT plans from all units across the RUBAVU District.
2. Develop and recommend RUBAVU District policy with relation to ICT.
3. Review and recommend on ICT project development plans within the context of ICT plans.
4. Create ad hoc committees to address strategic ICT issues, as required.
5. Review, coordinate and arbitrate major ICT activities across the District.
6. Provide an annual report to District Executive Committee that details ICT activities.
7. Report to District Executive Committee at each necessary.

II.2.3 MEMBERSHIP

- Deputy Mayor in charge of Economics affaires
- District Executive Secretary
- Representative of Sector Executive Secretaries -
  Director of administration
- Director of Monitoring, Planning and evaluation
- Director of Finance
- ICT Officer
- Permanent Secretary JAF
- Lawyer & Notary
- Public relation Officer

II.2.4 MEETINGS

The committee meets approximately every quarter of the financial year. Additional meetings will be called when necessary. Prior to being put forward to the District Executive Committee, decisions and/or recommendations are finalised through consensus of the committee members.

II.2.5 REPORTING

Major recommendations are sent to the District Executive Committee for approval.

II.2.6 SUPPORT

- Administrative support is provided by Monitoring, Planning and Evaluation Unity.
- Minutes for the meetings are taken by Network and System Administrator or PRO.

II.2.7 FURTHER DELEGATION OF AUTHORITY

This committee has no delegated powers to another committee. ICT Steering Committee has the power to create subcommittees on an as-needed basis. These subcommittees are to report back to ICT Steering Committee with reviews and recommendations.

III. GOALS AND OBJECTIVES

III.1 IT STRATEGIC PLAN

The District IT steering committee must agrees on the decisions regarding IT and these decisions should be formalised and documented in the District Development Plan (DDS) of five years.

III.2 IT TACTICAL PLAN

The District IT tactical plan will be done on a yearly basis and will flows out of the District IT strategic plan in order to support the strategic plan to ensure that the District achieves the objectives defined in the strategic plan

IV. OWNERSHIP OF INFORMATION ASSETS

IV.1 OVERVIEW

Information assets is a definable piece of information, stored in a manner which is "valuable" to the organisation.

IV.2 CLASSIFICATION OF DATA

The District stores data on External hard disks, Server and Network attached device and these data are classified:

- **District Correspondance**: those are all outgoing and incomming letters to District and also emails files.
- **District database:** all data representing dailly life of the District
- **Employees files:** data concerning District Management employees
- **Employees Services data:** data which are related to service provided by employees.

IV.3 OWNERSHIP ESTABLISHEMENT FOR DATA

- **USERS:** all users will have account to the Server which will serve them to do regural back-up and access to data stored, those data will be stored according to departement the user is located.
- **Network and System Administrator:** The Network and System Administrator will have the right to manage user's access to data and management of all District data.
- **HR MANAGER:** Will have access to manage District Employees files
- **CENTRAL SECRETARIAT:** Will have access to manage District Correspondance

- **DISTRICT STATICIAN:** will access to manage all District database

- **DISTRICT ARCHIVIST:** will have access to all District data but not their management

V. SECURITY

V.1 PHYSICAL AND ENVIRONMENTAL SECURITY

The Server room located at RUBAVU District must be claused when is unoccupied and the District Software and Network System Administrator must hold the Key in order to control phyisical access to servers,switches,routers,cables and other devices located in that room.

If employees use laptops at their desks, they should take them with them when they leave or secure them with passwords in order to protect data to be stolen

In case of disaster, the District must install fire extinguisher s and lightning conductors at their buildings.

V.2 NETWORK SECURITY

The District Software and Network Administrator is responsible for installing antivirus in Employees Computers, the update of the antivirus is on charge of employees, The wireless network used must be secured with password in order to prevent people to connect to that network.

Network and System Administrator assisted by Broad Band system Corporation (BSC) is responsible for securing the District Network

V.5 BUSINESS CONTINUITY & DISASTER RECOVERY

Back up Procedures

This chapter provides procedures and practices that will be observed during all backup exercises. It covers the backup of the organization's servers only. Backup of all user workstations is covered in the district IS Policy. Backup of server will cover the transfer of all the below listed data to a Magnetic Tape or CD:

- Inventory Systems
- Server System State: includes the system registry, active directory, DHCP, DNS and WINS settings, all other systems settings.
- MS Exchange: includes Exchange server settings and all user e-mails.
- Applications: all exe, dll and ocx files.
- User files

Media used will always be DDS4 20/40 GB magnetic tapes or CD.

Backups will be taken at different intervals and times depending on what is being backed-up. The following procedures will be observed during backup of each of the above listed data.

Guideline	Description and Applicable procedures
System State, User Files and Storage Backup	All the above will be backed-up at the end of each working day. These contain the data with the highest number of changes regularly. This will ensure that all the system, user files and database changes made during the day are archived at the end of each day. To ensure quick recovery of data in the case of a break down the following procedure is to be observed during archiving: • Every Friday a normal backup is taken of all the above. This backup set will be sent to Head Office for safe storage after sign-off. • Monday through Thursday a differential backup is taken of all the above. This will backup only the newly created or changed settings and files. • A daily-automated backup of the Storage databases will be setup to backup the Applications and Databases into a specified folderon the storage-server for each department and with subfolders inside for the department employees to back up.
MS-Exchange Backup	The Organization‟s email service runs on Ms-Exchange 2010. These will be backed-up once every two days. The backup taken will always be a normal backup on a single or multiple tapes ensuring all e-mails are archived.
Application Files Backup	All exe, bat, dll and ocx files which are required for the running of applications will be backed-up once every month or once a change or patch is applied. This will be a normal backup every time it is performed.

Backup Testing and Review	All backup tapes will be tested both manually and automatically. A periodic manual test will be performed by ICT service personnel and confirmed by the relevant Manager. A testing log will be signed to confirm success or failure of the backup media. The user files, system state and database backup will be given the highest priority in testing. The system will be configured to perform an automatic test of the media after completion of all backup processes. A report is normally generated by the system after every test; this will be printed and signed by the Revenue Assurance Manager for filing. The Management will review all backups performed periodically and confirm by signing of their validity and integrity All the above documents will be filed for future reference.
Backup Logs	These will be printed from the System everyday and signed off by one I.T. personnel and the DAF. Signed copies will be stored in the „Back up logs‟ file for future reference.