**WORKFORCE DEVELOPMENT AUTHORITY – WDA**
*Empowering people with employable skills and entrepreneurship capacity*
**P. O. BOX 2707**
**Tel: (+250) 255113365**
**E-mail: info@wda.gov.rw**
**Website: www.wda.gov.rw**

# INFORMATION SECURITY POLICY

## Table of Content

## EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies and IT equipment of Workforce Development Authority and the framework/structure required to communicate, implement and support these policies. Information is an asset, which like any other asset owned by the Institution, has significant value to the stakeholders of the Government. Information security is a critical component that is required to enable and ensure the availability, integrity and confidentiality of data, network and processing resources required for the institution to perform its business and operational practices. This policy document has been developed to establish and uphold the minimum requirements that are necessary to protect information resources (assets) against unavailability, unauthorized or unintentional access, modification, destruction or disclosure.

Common best practice for information security management dictates the following essential controls:

1. Data protection and privacy of personal information;
2. Safeguarding of organizational records;

- **Controls for information security:**

1. Information Security Management Policy document;
2. Allocation of information security responsibilities;
3. Information security education and training;
4. Reporting procedures for security incidents;
5. Business continuity management.

The scope of this document is intended to cover any information asset owned, leased or controlled by the WDA and the methodologies and practices of external entities that require access to the Institution's information resources. These assets include hardware, software, data and information.

This document applies to all full- and part-time employees of WDA and all third parties, contractors or vendors who work on WDA premises or remotely connect their computing platforms to the Institution's computing platforms.
By establishing the appropriate policy framework and utilizing a documented policy development process that includes all stakeholders, the Government envisions maximum voluntary compliance.

## CHAPTER 0: INTRODUCTION

### 0.1. What is Information security?

Information, although generally intangible, is an asset like any other business asset and has a value to an organization, which consequently needs to be suitably protected; also, there are confidentiality, integrity and privacy issues (possibly legislated) that need to be considered. Information security is necessary to protect information from a wide range of potential threats in order to ensure business continuity, minimize business damage and maximize return on the considerable investment required to gather, maintain and process information.

Information exists in many forms. It can be printed or written on paper, stored electronically and transmitted by various means. Whatever forms the information takes; it needs to be appropriately protected.

Information security is categorized as the preservation of:

- **Confidentiality: ensuring that information is accessible only to those authorized to have access;**
- **Integrity: safeguarding the accuracy and completeness of information and processing methods; and**
- **Availability: ensuring that authorized users have access to information and associated assets when required.**

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software functions. These controls need to be established to ensure that the specific security objectives of the organization are met.

included in this document are to be considered the minimum requirements for providing a secure operational environment.

## 0.2. Assessing security risks

Security requirements must be identified through a process of methodical assessment of security risks. Expenditure on controls needs to be balanced against the business harm likely to result from security failures. Risk assessment techniques may need to be applied to the organization as a whole, or to only parts thereof, as well as to individual information systems, specific system components or services where this is practicable, realistic and helpful.

Risk assessment is the systematic consideration of:

- **The business harm likely to result from a security failure, taking into account the potential consequences of a loss of confidentiality, integrity or availability of the information and other assets;**
- **The realistic likelihood of such a failure occurring in the light of prevailing threats and vulnerabilities, and the controls currently implemented.**

The results of such an assessment will determine the appropriate management action - and priorities - for managing information security risks, and for implementing controls selected to protect against these risks.

Periodic reviews of security risks and implemented controls are essential to:

- **Take account of changes to business requirements and priorities;**
- **Consider new threats and vulnerabilities;**
- **Confirm that controls remain effective and appropriate.**

Assessment of risk is therefore not a singular event but a regular cycle that needs to be implemented and managed.

# CHAPTER 1: ACCEPTABLE USE POLICY

## 1.1. General Requirements

- End-users are responsible for exercising good judgment regarding appropriate use of Institutional resources in accordance with Government policies, standards, and guidelines.
- For security, compliance, and maintenance purposes, authorized personnel shall monitor and audit equipment, systems, and network traffic.
- Devices that interfere with other devices or users on the Institution network may be disconnected.
- The ownership assigned to the user of the information assets and information processing facilities should be approved and reviewed regularly.
- Users must not purposely engage in activity that may: harass, threaten or abuse others; degrade the performance of Information Resources;; obtain extra resources beyond those allocated; circumvent Government computer security measures.
- Institutional Information Resources must not be used for personal benefit.

## 1.2. Information Classification

- The Classification Categories are:
  - Strictly Confidential
  - Confidential
  - Internal
  - Public
- It is the responsibility of the asset owner to define the Classification of the asset, periodically review it, and ensure it is kept up-to-date and at appropriate level.
- The asset owner may also specify the access rights / approve authorization of user to access the asset.
- It is responsibility of the information users to ensure compliance to the defined categories.

### 1.3. Password Use

- User will not keep copy of password in any written form or electronic form. If absolutely required, passwords of critical user accounts shall be maintained securely.
- Users will change passwords whenever there is any indication of possible system or password compromise.
- Users will change Passwords at regular intervals 90 days or based on the number of access (passwords for privileged accounts should be changed more frequently than normal passwords), and avoid reusing or cycling old passwords.
- Users will change temporary passwords at first logon
- Users must not include password in any automated logon process, e.g.: stored in a macro or function key
- Users will not share their passwords with anyone
- Users will ensure that nobody is watching when the password is being entered
- Wireless access points shall be secured with help of a security key

### 1.4. Password construction

- Users should choose passwords that are easy to remember but difficult to guess. Some of the guidelines for password constructions are:

  - Quality password with sufficient minimum length 8 Characters long
  - Easy to remember
  - Not based on anything, somebody else could easily guess or obtain using persons related information (e.g.: Names, Telephone No's, Date of Birth, Company Name, Spouse Name etc.)
  - Not vulnerable to dictionary attack (i.e. do not consists of words included in dictionaries)
  - Free of consecutive identical, all-numeric or all alphabetic characters
- Do not use word or number patterns like aaabbb, qwerty, zyxwvuts,123321, etc
- Not use the same password for business and non-business purposes
- Strong passwords would have a minimum length of 8 characters and can be constructed through a mix of numerals (1,2,3 etc), special characters (!,@,#,$ etc) and capital letters (A,B,C etc).
- One way to create complex but easy to remember passwords is to take a known word or passphrase and convert it using numerals, special characters and capital letters. For example, the passphrase/word might be "complex" and password could be: "c0mp1@x".

  **NOTE**: Do not use either of these examples or any examples given in seminars, workshops, training etc. as your passwords.

### 1.5. Unattended User Equipment, Clear Desk and Clear Screen

- All users are responsible for implementing security procedures for protecting unattended equipment's.

- All users shall terminate active sessions by using Ctr+Alt+Del and then Enter when there is a need to step away from the system.
- Sensitive or critical business information, e.g.: on paper or on electronic storage media, should be locked away when not required, especially outside the normal working hours.
- Computers and terminals should be left logged off or protected with a screen and keyboard-locking mechanism controlled by a password when unattended and should be protected by key locks, passwords or other controls when not in use.
- Incoming and Outgoing mail point and unattended machines should be protected
- Unauthorized use of photocopiers and other reproduction technology like scanners, digital cameras, should be prevented.
- Documents containing sensitive or classified information should be removed from printers immediately.
- System administrators shall ensure that the active directory system is configured to automatically lock systems, which are inactive for more than 5 minutes.

### 1.6. Information exchange Policies and Guidelines

- Appropriate controls will be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.
- End-users will,
  - Not leave sensitive information unattended at fax machines, printers etc.
  - Not auto-forward mails to external mail ids.
  - Not reveal sensitive information in public.
  - Not leave sensitive messages on answering machines.
  - Check the recipients email id/fax number before sending an email or a fax respectively.

### 1.7. Reporting Information Security Incident and Weaknesses

- All employees, contractors and third party users of WDA should be aware to report any information security incidents in systems or services

### 1.8. Prevention of misuse of information processing facilities

- All employees, contractors and third party users of the institution should use the information processing facilities for business purposes only.
- Any use of these facilities for non-business purposes without management approval or for any unauthorized purposes, should be regarded as improper use of facilities or breach of confidentiality.
- Intrusion detection, intrusion prevention, content inspection, and other monitoring tools shall be used to detect and prevent misuse of information processing facilities.

### 1.9. Anti-Virus

- All workstations and laptops will have anti-virus installed, running and updated. A corporate anti-virus should be implemented in the Institution.

- All hosts used by the employee that are connected to the Institution Internet/Intranet/Extranet, whether owned by the employee or by the Institution shall have approved virus-scanning software with a current virus database.
- User will not change the anti-virus settings.
- Users should not disable the installed anti-virus agent or change its settings defined during installation. This includes settings for daily virus scan; anti-virus server address and signature update schedules.
- Users should not disrupt the auto virus scan scheduled on their desktop. If the scan is affecting system performance, users should contact system administrator for resolution.
- All external media will be used only after authorization and subjected to anti-virus scan and users are advised to run anti-virus scan when any external media is used.
- Users will report any virus detected in the system to ICT Unit or to a reporting manager within respective department
- Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- Users should exercise caution when copying files. Only download from reputable sites, and carry out a virus check on the file.

## 1.10. Internet Usage

- Users shall not use or access the internet for non-business purposes and restrict personal use to minimum limited to educational, knowledge and news sites. Users should strictly avoid visiting non-business, offensive and unethical sites which violate security policies.
- Users should not use Internet facilities to:
  - Download or distribute malicious software or tools or to deliberately propagate any virus
  - Violate any copyright or license agreement by downloading or distributing protected material
  - Upload files, software or data belonging to WDA to any Internet site without authorization of the owner of the file/ software/ data
  - Share any confidential or sensitive information of WDA with any Internet site unless authorized by Superior / Management
  - In case such misuse of the Internet access is detected, Authorized personnel shall terminate the user Internet access and take other disciplinary action.
  - Users should ensure that they do not access websites by clicking on links provided in emails or in other websites. When accessing a website where sensitive information is being accessed or financial transactions are done, it is advisable to access the website by typing the URL address manually rather than clicking on a link.
- Users must be aware that WDA accepts no liability for their exposure to offensive material that they may access via the Internet.
- Users should ensure that security is enabled on the Internet browser as per guidelines given below-
  - Configure browser not to remember web application passwords.
  - Set browser security setting to medium.

- WDA reserves the right to monitor and review Internet usage of users to ensure compliance to this policy.

### 1.11. User Privacy

- Users should have no expectation of privacy while using company-owned or company-leased equipment. Information passing through or stored on company equipment can and will be monitored as and when required for security and compliance reasons.

### 1.12. Email Usage

- Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.
- Users shall comply with Institution's e-mail policy on proper and effective use of e-mail.
- WDA has the authority to intercept or disclose or assist in intercepting or disclosing email communications.
- Users will not use any email account other than the one provided by the institution for transacting official information.
- Confidential information will be secured before sending through e-mail by way of compression, password protection or other advanced cryptographic means.
- Language used should be consistent with other forms of business communications
- WDA employees should treat electronic-mail messages with sensitive or confidential information as 'Confidential' and take due care as per the' information handling guidelines'.
- Users shall avoid opening mail from unknown users/sources and also avoid opening suspicious attachments or clicking on suspicious links.
- Users shall avoid any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Users shall avoid unauthorized use, or forging, of email header information.

### 1.13. Laptop Security

- Laptop users should take additional responsibility for the security of their laptop and the information it contains. Users should adopt the following measures and consult ICT Unit for any clarification,
  - Ensure that laptop is configured as per the secure configuration. Do not install unlicensed or doubtful software/ applications.
  - All sensitive data on laptop should be secured either through password protection or by using encryption.
  - Whenever connecting to the LAN, ensure that anti-virus agent is installed with latest signatures on the laptop.
  - Log off laptops when not working for extended period and enable screen saver with password for protection during short period of inactivity.
  - Backup critical files from laptop on the network location.
  - Take adequate measures for physical protection of laptop including not leaving laptops unattended in public places or while travelling.

- Personal Digital assistant (PDAs) devices, laptops, wireless phones and miniature hard drives will not be connected to the LAN without prior permission from the reporting manager.
- If the laptop has modem/ dial up facility for Internet, users should disconnect Internet connection before connecting to LAN. Users having dialup facility are recommended to have personal firewall installed to prevent unauthorized access to their laptop while connected to Internet.

➢ Loss of laptop should be reported immediately to Admin Dept / ICT Dept.
➢ In case any laptop is connected to the company network without authorization, the ICT / Security Department shall take appropriate action against it.

### 1.14. Exchange Agreements

➢ In case of an exchange of information between WDA and an external party, appropriate agreement will be established addressing the following points:
- Traceability and non-repudiation
- Courier identification standards
- Responsibilities and liabilities in the event of an incident
- Labeling system as per the sensitivity of the information
- Cryptography

## CHAPTER 3: ASSET MANAGEMENT POLICY

WDA should ensure that all information and information processing assets are identified, classified and adequately protected by the owners of these assets. It should also ensure that boundaries of acceptable use are clearly defined for anyone that accesses any of the information assets.

### 3.1. Inventory of assets

"All assets should be clearly identified and an inventory of all important assets drawn up and maintained."

➢ ICT Unit/administration shall ensure Inventory of all information assets are drawn and maintained with each department.
➢ The asset inventory shall include type of asset, owner, location, backup information, license information and the asset sensitivity value based on Confidentiality, Integrity and Availability. (type of asset are 'Hardware, software, information, service, people, etc)
➢ Respective Information asset owners will classify, label and handle information based on the classification scheme and guidelines
➢ Respective Information owner shall note in the asset inventory all the critical information assets required to be recovered in a disaster.

### 3.2. Ownership of assets

"All WDA information and assets associated with information processing facilities should be owned by a designated department"

- Each information asset will have an identified owner who will be responsible for safeguarding the asset
- The respective information owners shall be responsible for assigning and maintaining appropriate information classifications based on the information classification schemes.
- Respective Information owner shall be responsible for deciding the allocation of access rights and classifications of the Information assets.
- Respective Information owners shall review access to information assets every quarter.
- Respective Information owners shall review information classification of the asset inventory at least once a year.

### 3.3. Acceptable use of assets

"Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented"

- Information Security Implementation Team shall ensure all employees, contractors and third party users follow Information assets acceptable usage guidelines.
- ICT Unit and HR shall be responsible for communicating acceptable usage guidelines to all employees, contractors and third party users at the time of engagement with the organization.

### 3.4. Classification guidelines

"All Institution information should be classified and secured in terms of its value, legal requirements, sensitivity and criticality "

- The Administration Unit shall ensure that a procedure for defining, allocating and reviewing information classifications is documented.
- The designated information asset owners shall classify all assets as per the classification schemes specified in information security guidelines.
- Respective Information owners shall review access and classify critical information
- All users shall classify information as per the information classification procedure.
- Asset owner shall take due care of classifying and maintaining contracts of clients.
- All Institution information shall be treated as confidential.
- Respective Information owners shall ensure access is based on need to know basis (Read, write access based on individual role)

### 3.5. Information labelling and handling

- The ICT and Admin Unit shall ensure all assets are labelled using asset tags.
- Employees shall be made aware of their responsibilities regarding handling of sensitive information.
- Information no longer useful shall be permanently deleted from the system.
- All critical information shall be securely protected (Files shall be password protected, critical information shall be encrypted.
- Media with confidential information shall be physically labelled.
- Users shall ensure all paper information no longer needed shall be shredded
- Media tapes shall be stored in lock and key at all times
- Backup media shall be labelled and stored in locked fireproof cabinets.
- Media in transit shall be securely stored using bubble wraps or boxes.

## CHAPTER 4: PERSONNEL SECURITY POLICY

*The objective of this policy is to ensure that employees of WDA understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risks of human error, theft, fraud or misuse of facilities and address security responsibilities prior to and during employment.*

Security responsibilities should be addressed at the recruitment stage, included in contracts, monitored during an individual's employment, and considered during contract termination process.

### 4.1. During employment

- Appropriate awareness trainings and regular updates on organizational policies and procedures will be provided to all WDA employees, Contractors and Third party users of the organization as relevant to their job functions. Awareness training will continue to be part of the induction process.
- All WDA employees, Contractors and Third party users are required to follow the information security policies and procedures.
- A formal disciplinary process will be initiated against employees violating laid down policies and procedures or perpetrating security breach. This may include termination of employment or legal action.

### 4.2. Termination or change of employment

- HR department in conjunction with the concerned head of department will follow a termination / change in role process.
- In case of termination, a clearly defined exit procedure will be followed and a record of the same will be maintained. This will include the return/review of all previously issued information and information processing assets.
- The access rights of all employees and contract employees to information and information processing facilities will be removed on termination of their employment / contract / agreement or modified for any change in their designation / status.
- All employees, contractors and third party users should return all WDA assets in their possession upon termination of their employment, contract or agreement.
- HR department will ensure that all the assets of the organization e.g. Service ID cards, laptops are returned by the outgoing employee or contract employee upon termination of their contract or at the end of employment.

## CHAPTER 5: PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

*The objective of this policy is to prevent unauthorised access, damage and interference to business premises and information.*

It is essential that critical information processing facilities are housed in secure areas, protected by a clearly defined security perimeter, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference, commensurate with the identified risks. The practices of "clear desk" and "clear screen" should be encouraged to reduce the risk of unauthorized opportunist access to facilities.

### 5.1. Physical Security Perimeter

- Security perimeter for the office premises, server rooms, and other sensitive business areas will be defined to form a physical boundary
- Different areas of the Institution will be categorized under following classifications:
  - Green Zone - Areas accessible to public e.g. Reception
  - Blue Zone - Areas not accessible to public but accessible to all employees
  - Red Zone - Secure Areas. These are like the Data center/Server rooms, network equipment's rooms,...
- All entrances and exits to the premises will be manned 24x7 and red and blue zones will have an access card system
- Red zone will have motion sensors or CCTV camera implemented to detect any unauthorized movement. All entrances / exits to red zone areas and blue zone areas, all green zone areas will be monitored though closed circuit television (CCTV) systems.
- Red zone will have a two factor authentication system over and above proximity card access control system.
- Fire doors and emergency doors will be alarmed, monitored and tested every quarter
- All the critical or sensitive information processing facilities shall be housed in secure areas
- An entry / exit log for all the visitors entering blue zone and red zone areas will be maintained
- Visitors to red zone areas will be escorted throughout their stay
- Visitors will be asked to declare their belongings at entry and this will be verified when the visitors exit
- A separate list of external party personnel who require long term access will be maintained
- All personnel entering blue zone or red zone areas will be required to wear a visible identification.
- All WDA Employees, Contractors and third part users are required to wear an Institution's Identification
- A list of personnel having access to red zone areas will be maintained. Access rights to red zone areas will be reviewed on a quarterly basis
- All delivery will be received in green zone areas. If access to blue zone or red zone areas is required, the delivery personnel will be escorted throughout their stay.
- Photographic, video, audio or other recording equipment, such as cameras in mobile devices, should not be allowed in red zone, unless authorized by the ICT Unit/Administration.

### 5.2. Environmental Security

- The backup files and sensitive paper documents will be kept securely off-site. The backups will be stored in appropriate environmental conditions as per the manufacturers' specifications taking into account air conditioning, humidity etc.
- Fire detection and suppression systems will be installed to safeguard Institution assets against fire.
- WDA will ensure that the security personnel and personnel often working in the secure area are trained in using fire extinguisher equipment.
- The power supply equipment, air-conditioning and other equipment will be protected from disruptions, power surges. All such equipment will be under annual maintenance contracts with service level agreements.
- Cabling (Power and telecommunication) carrying data or supporting information services should be properly labeled (point to point) with necessary identification methods and protected from interception or damage
- power and telecommunications lines into information processing facilities should be underground, where possible, or subject to adequate alternative protection;
- All critical equipment will be adequately insured.
- All organizational physical security systems should be properly managed by both Admin department and ICT department to effectively and securely operate them.

# CHAPTER 6: COMMUNICATION AND OPERATIONS MANAGEMENT POLICY

All the information, its communication and processing facilities, flow of information within WDA and outside institutions will be protected by appropriate system / network planning, management and through well-established operating procedures.

## 6.1. Operational procedures and responsibilities

*Documented Operating Procedures*

- Operating procedures for information systems will be documented and authorized by the management and will be made available to all users who need them. These procedures include:
  - Server and networking equipment start up and close down
  - Backup
  - Equipment maintenance
  - Media handling, computer room and mail handling management, and safety.
  - Operating procedures require specifying the instructions for the detailed execution of each job including the interdependencies, if any, and instructions for dealing with exceptions or errors that may arise during job execution.

*Change Management*

- Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment, applications and procedures are required to be followed.
- Change management form needs to be completed for each scheduled, unscheduled or emergency change following the steps contained in the Change Management Procedures.
- A Change Review must be completed for each change, whether scheduled or unscheduled, and whether successful or not.
- A Change Management Log will be maintained for all changes. The log must contain, but is not limited to:
  - Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change
  - Indication of success or failure

*Segregation of Duties*

- Roles and responsibilities will be assigned, implemented and reviewed for each critical process.
- Due care will be exercised to segregate the roles and responsibilities. Wherever it is practically not feasible to segregate the roles and responsibilities, appropriate supervision will be carried out.

*Separation of development, test, and operational facilities*

- The Network Administrator shall ensure that there is separation of development, test and production environment for all the changes to the operational systems.

- The system Administrator shall ensure that utilities like compilers, editors and other development tools or such systems utilities are removed from the production system.
- The IT Administrator shall monitor and control the access to the utilities.
- The Testing team shall ensure that sensitive data is not copied into the test environment.
- The IT Administrator shall ensure that users are given different user profiles for operational and test facilities.
- The IT Administrator shall ensure that the installation of software on its production systems to prevent corruption of systems and information is controlled.

### 6.2. Protection against Malicious and Mobile Code

*Controls against malicious code*

"Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures shall be implemented"

- To prevent the spread of and exploitation by malicious code, the IT System shall be configured to prevent users from installing unauthorized software.
- The IT Systems Support team shall ensure that appropriate detective and preventive measures are implemented at key network locations to protect the organization against risks introduced by malicious code.
- The IT Systems Support team shall ensure that the anti-virus software is running the latest virus signatures.
- The IT Systems Support team shall ensure that all users log into their desktops using "normal user" privileges.
- All emails messages shall be scanned before entering and leaving the organization for presence of any malicious code.
- All users shall be trained on the best practices to be followed while using computer systems to prevent the outbreak of a virus incident.

*Protection and treatment guidelines*

Necessary technical and operational procedures will be in place for centralized Antivirus definition updates.

- It will be ensured that the Anti-virus software is installed and active on every machine. The configuration of Anti-Virus software will be protected to avoid any unauthorized modifications.
- Updating of anti-virus definitions on all computers will be managed centrally.
- Systems will be implemented to review the anti-virus software activity / logs, to check whether anti-virus software is running regularly on respective computers.
- Machines will be scanned for virus at least once in a day and it will be properly scheduled, preferably during the lunch hours of the office.
- Every storage media shall be scanned for virus before use.
- Controls will be implemented to protect the network from spyware software.
- The Anti-Virus software for messaging system (e-mail) will be implemented. If the virus is found in mail attachment file, this file will be deleted and the sender will be informed. The recipient would get the remaining message.
- Users will be regularly updated about the latest information on malicious code through circulars, internal communication mail etc.
- Unauthorized or any pirated software will not be used by the WDA employees.

- Any files or data obtained from outside through any media required for business, will be tested for virus before being used.
- Necessary procedural protection will be taken to protect against the introduction of malicious code during maintenance and emergency procedures, which may bypass normal malicious code protection controls.

### 6.3. Back-up

*Information backup and archival*

"Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy"

- The ICT Unit shall maintain a record of all data that needs to be backed up along with the schedule for each.
- The ICT Unit shall ensure that backup logs are reviewed on a daily basis.
- The ICT Unit shall ensure that all backup tapes are moved to an offsite location on a daily basis.
- The ICT Unit in co-ordination with the Administration unit shall ensure that all backup equipment and tapes are given adequate physical protection, both onsite and off-site.
- The ICT Unit shall test all backup media once a month to test the completeness of the backup.

### 6.4. Network security management

*Network Controls*

"Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit."

- Overall responsibility for network activity will be clearly assigned to an individual (i.e. the network 'owner'). Responsibilities for key tasks will be assigned to one or more individuals who are capable of performing them.
- The risk of staff disrupting the running of the network either in error or malicious intent will be reduced by:
    - Segregating the duties of staff running the network. In case practically not feasible, incorporating suitable audit trail and quarterly review of the activities.
    - Ensuring all network and external staff sign non-disclosure/confidentiality agreements
    - Minimizing reliance on key individuals (e.g. by automating tasks, ensuring complete and accurate documentation, and arranging alternative cover for key positions)
    - Organizing duties to minimize the risk of theft, fraud, error and unauthorized changes to information (e.g. by supervising and recording activities, prohibiting lone working and the segregation of duties)

*Security of Network Services*

- The IT Manager shall ensure that sufficient technology controls are implemented whilst taking security/network services from a service provider. The controls shall take into account the confidentiality, integrity and availability of the data being transmitted between the client and the service provider.

- The ICT director shall ensure that Operational Level Agreements are signed with units providing network and security services.
- The ICT director shall regularly monitor the services provided by these unit/departments. Corrective and Preventive actions shall be carried out to ensure that these units/department provides services as agreed to in the agreement.

*Wireless communication security*

- Wireless router should be tested prior to selection, test should include but not limited to below points;
    - Inter compatibility with other network devices
    - Should support strong encryption and authentication protocol i.e.WAP2
    - Should have logging mechanism
- All access to wireless networks shall have strong authentication mechanisms to prevent unauthorized users.
- The SSID of the wireless device shall be configured in such manner so it does not contain or indicate any information about the organization, its departments, or its personnel including organization name, department name, employee name, employee phone number, email addresses, or product identifiers.
- WEP & WAP must not be used for Wireless deployment (These are vulnerable) only WAP2 with EAP-TLS.
- All file servers and internal domain controlling servers shall be separated from the wireless network using a firewall
- Wireless access to third parties shall only be provided after adequate verification and authorization.
- Default Administrator password on AP must be strictly changed…..

## 6.5. Media handling

*Management of Removable Media*

- Movement of media containing information will be supported by suitable authorization process.
- In case the confidential information needs to be printed on a common printer, then a responsible person will supervise while the information is getting printed and ensure that no printouts are left on the printer.

*Security of System Documentation*

- WDA will ensure that all system documentation is handled as per its classification.
- Access to system documentation shall be approved by Reporting manager to prevent possible data loss

> *"System Documentation" means those operational manuals, tables, access control lists, or other documentation that contain sensitive information such as the descriptions of application processes, procedures, data structures, addressing schemes, and authorization processes which if divulged could compromise the security of the systems referenced within such documentation.*

## 6.6. Exchange of information

*Information Exchange Policies and Guidelines*

"Formal exchange policies, procedures, and controls shall be in place to protect the exchange of information through the use of all types of communication facilities"

- Appropriate controls will be implemented for protection against malicious code, while transmitting information electronically.
- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- Disposal procedures will be followed to destroy sensitive information.
- End users will:
    - Not leave sensitive information unattended at fax machines, printers etc.
    - Not auto-forward mails to external mail ids.
    - Not reveal sensitive information in public
    - Not leave sensitive messages on answering machines

*Electronic messaging*

- Information present in electronic messages will be appropriately protected according to its criticality.
- Confidential Emails will be encrypted and attachments will be password protected for information passing over the publicly accessible networks.

## 6.7. Monitoring

*Audit Logging*

"Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring"

- System administrator will maintain Operational and Maintenance logs of all activities.
- The logging will be automated as far as possible. Implement automatic recording of logs wherever feasible as it is useful to maintain integrity of the logged information. Logs will include, but not limited to:
    - Date, time and other details of key events, e.g. log-on and log-off
    - Records of successful and rejected system access attempts
    - Changes to system configuration
    - Use of privileges
- All activities of system administrator / system operator will be logged and reviewed at least once in a quarter by the responsible person.

*Fault Logging*

"Faults shall be logged, analyzed, and appropriate action taken"

- Users will report problems encountered with information systems and communication systems to the system administrator.
- The faults reported will record the nature of problem, date and time of the report and user identity.
- System administrator will initiate proper process to resolve the faults recorded. ICT Director will authorize the corrective action.
- The details of action taken will be recorded along with date and time of action and person performing the action.

*Protection & Retention of Logs*

- Logs will be protected from unauthorized accesses and changes.
- Logs will be backed up daily/weekly. These logs will be archived quarterly.

- The log retention period will be determined based on business needs, legal and contractual obligations.

*Monitoring System Use*

- It is essential to monitor the use of information systems to safeguard the information from unauthorized activities.
- Level of monitoring will be determined by risk assessment of individual systems.
- Review of event logs is an important function in monitoring system use. System administrator will monitor their respective systems daily and report any unauthorized activity noticed.

*Clock Synchronization*

- The correct setting of computer clocks is important to ensure accuracy of logs. The logs may be required for investigations or as evidence in legal or disciplinary process.
- All information systems and devices, which have real time clocks, will be set to Rwanda Standard Time Zone.

# CHAPTER 7: ACCESS CONTROL POLICY

Access to WDA information processing facilities, application systems, databases, network, communication and operating systems will be restricted on business need basis to ensure confidentiality, integrity and availability of its information.

## 7.1. User registration

- All users will have a unique identifier (user ID) for their personal and sole use so that his / her activities can subsequently be traced to assign responsibility for actions or in case of any system misuse.
- The level of access granted to each user will be based on business requirement only..
- A formal record of all persons registered to use the information systems will be maintained.
- Access rights of all users who have changed roles/jobs or have left the organization will be revoked immediately. In certain cases where the user ID or account needs to be maintained for a certain period, sufficient controls will be put in place to prevent any misuse.
- The information systems will be checked on a quarterly basis to ensure redundant user IDs and accounts do not exist.

## 7.2. User Password Management

- All users will be required to keep personal passwords confidential.
- All newly created user IDs will be assigned a temporary password which will be changed immediately upon first logon.
- Any user requesting a change in password will be duly verified.
- Temporary password will follow the complexity rule.
- Default vendor passwords will be changed or disabled following the installation of the system or software.

## 7.3. Review of user access rights

- User access rights will be reviewed at least once in a quarter and after any change in employment of the user such as promotion, demotion or termination by the respective reporting manager.
- Privileged user access rights will be reviewed quarterly.
- Necessary controls such as removal of extra access rights will be conducted in case of any ambiguity found during the review.

### 7.4. User Responsibilities - Password Use

- All users including agencies working within WDA premises will be trained to keep passwords confidential and not share it with anyone.
- If there is an indication of a possible system or password compromise, the password associated with the concerned system will be changed immediately.
- Passwords of information systems will be of a minimum length of 8 characters.
- The characters in the password will be a combination of numeric, alphabetic and special characters.
- The passwords will be difficult to guess or derive and towards this end will avoid using personal information such as names, telephone numbers, date of births etc.
- Passwords will be changed every 90 days.
- Password history will be maintained for 5 past used passwords.
- All temporary passwords will be changed at first log-on.
- Passwords in any automated log-on process will be avoided.

### 7.5. Clear desk and clear screen policy

- All sensitive documents and storage media containing sensitive documents will be locked away when not required and especially when the office is vacated.
- All sensitive documents being printed will be immediately removed from printer areas to prevent unauthorized access.
- The organization will make use of shredder systems to get rid of paper documents that may no longer be required or left unattended near printer areas.
- All computer screens will be set to lock automatically after 5 minutes of inactivity.
- All computer screens will be locked when left unattended.

### 7.6. User authentication for external connections

- Strong Authentication mechanism must be implemented to control external and Internal connections to WDA networked services e.g VPN techniques,

### 7.7. Equipment identification in networks

- The ICT Director shall ensure that connection to network devices for administrative purposes is identified through an IP Address or MAC Address.
- The ICT Director shall ensure that all network devices are configured to control access to and from the network using identifiers such as IP Addresses or MAC Addresses
- Any new devices connected to WDA networks shall be identified and monitored

### 7.8. Segregation in networks

- The Network administrator shall ensure that a risk assessment is performed to analyse the security requirements of the network and the need to segregate the same into various domains.
- The Network admin shall ensure that the criteria for segregation of networks are based on the business needs for access control and security access requirements.
- The Network admin shall ensure that access controls are implemented between the various domains.

### 7.9. Network Connection Control

- The Network admin shall ensure that access control rules are implemented on the network devices to ensure that users access to information services such as email, file transfer, etc. are controlled.
- Where possible the Network admin shall ensure that Internet services are restricted and available during office hours only.

### 7.10. User identification and authentication

- The ICT Unit shall ensure that all the users have a unique user ID.
- The ICT Unit shall ensure that prior management approval is taken for creating shared user ID and generic ID.
- The users shall ensure that a strong password is used for authentication.
- The ICT Unit shall ensure that privileged IDs are created only after authorization from the Head of the department/ unit. Privileged IDs shall be different from those used for normal business use.

### 7.11. Session time-out

- The ICT Unit shall ensure that all computing equipment's are configured to lock after 5 minutes of inactivity.
- The ICT Unit shall ensure that wherever feasible, all inactive sessions are configured to shut down after a period of 10 minutes.

### 7.12. Limitation of connection time

- The ICT Unit shall enforce restrictions on connection time for sensitive applications to normal office hours if there is no requirement for over-time or extended-hours of operation.
- The ICT Unit shall enforce re-authentication at timed intervals.

### 7.13. Mobile Computing and Communications

- All users using mobile computing devices such as laptop, smart phones, iPad and similar hand held devices for business purposes shall be trained on the security best practices towards these devices. This training could be part of the end user awareness training conducted annually for all employees.
- A risk assessment shall be performed on the potential threats associated with the various forms of mobile computing for new devices that become available.
- Users of mobile computing devices (i.e. Laptop, smart phones, iPad and similar hand held devices) shall be required to sign a statement of their understanding and compliance to the mobile computing policy. This statement should be included in the policy acceptance letter signed during orientation.
- Users shall reasonably ensure mobile devices are physically secure at all times if they contain Institution sensitive data. Examples of physically securing devices include:
  - Mobile devices should never be left visible in a car, and should never be left in the trunk or other storage location overnight.
  - Mobile devices should always be carried on-board aircraft and not put in checked luggage
- If a mobile device contains other than Institution data, it shall have some form of access control (e.g. username and password) to access this information. If access to the device is not controllable, access to the data must be controlled.

- If a mobile device contains sensitive Institution data, it shall be encrypted on the storage drive. Encryption may be on a file-by-file basis, or on a volume-by-volume basis.
  - Users are strongly encouraged to back up their Institution data stored on mobile devices. Backup may be done when connected to the WDA network (file shares and other backup facilities), or may be backed up to removable media. If backed up to removable media, this media must be physically protected or the data must be encrypted.
- Remote connections to the WDA network shall be made from mobile devices at public places only after obtaining prior approval from the respective unit and Infrastructure Owner.
- Before connecting to the company network from the public network, the following points shall be considered:
  - Users must use an approved personal firewall, and have it running and actively filtering traffic, when connecting to WDA networks from public places.
  - Users must also have current and active anti-virus software running before connecting.
  - Remote connections will be made through VPN tunnels to safeguard the connection traffic.

## BUSINESS CONTINUITY POLICY

A practical and well-defined Business Continuity Plan (BCP) will be prepared to ensure that adequate procedures are in place to recover from disasters and resume normal business operations in the institutions. Recovery teams will be formed with clear, well – defined roles and responsibilities, to safeguard Personnel and Property in case of any disaster. There will be the need to identify critical functions, emergency response team with contact details and ensure that a well-documented BCP is in place. The plan must be maintained current and tested / exercised regularly.

- BCP personnel shall ensure the user awareness on emergency procedures is conducted once every year.
- Shall ensure roles and responsibilities for handling crisis situations shall be documented and communicated to relevant teams.
- The business continuity plans include established emergency procedures and existing fallback arrangements for all critical services.
- A business continuity framework shall be designed that states the conditions for activation and personnel responsible for execution of each component of the plan.

**Prepared by:**

**ICT Unit**

**Workforce Development Authority**