RWANDA POLYTECHNIC

P O Box 164, Kigali
Address: KK 15 Road, Kigali
Website: www.rp.ac.rw
Email: info@rp.ac.rw

INFORMATION SECURITY POLICY

EXECUTIVE SUMMARY

The main purpose of this document is to define the information security policies and IT equipment of Rwanda Polytechnic and the framework/structure required to communicate, implement and support these policies.. This policy document has been developed to establish 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 RP 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 RP and all third parties, contractors or vendors who work on RP premises or remotely connect their computing platforms to the Institution's computing platforms.

CHAPTER 1: INTRODUCTION

1.1. What is Information security?

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.

1.2. Assessing security risks

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.

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.

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 institution policies, standards, and guidelines.
- Users must not purposely engage in activity that may: harass, threaten or abuse others;
- Institutional Information Resources must not be used for personal benefit.

1.2 Information Classification

The Classification Categories are:

- Strictly Confidential
- Confidential
- Internal
- Public

1.3 Password Use

- User will not keep copy of password in any written form or electronic form.

- Users will change passwords whenever there is any indication of possible system threat 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
- 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
  - 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).

1.5 Unattended User Equipment, Clear Desk and Clear Screen

- 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
- Computers and terminals should be left logged off or protected with a screen and keyboard-locking mechanism controlled by a password.
- 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.
- 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.

1.7 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.

1.8 Anti-Virus

- All workstations and laptops will have anti-virus installed, running and updated.
- 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 disable the installed anti-virus change it's settings.
- All external media will be used only after authorization and scanned.
- Users will report any virus detected in the system to ICT Unit.

1.9 Internet Usage

- Users shall not use or access the Internet for non-business purposes. Users should strictly avoid visiting non-business, offensive and unethical sites.
- Users should not use Internet facilities to:
  - Download or distribute malicious software or tools or propagate any virus
  - Upload files, software or data belonging to RP to any Internet site without authorization of the owner of the file/ software/ data
  - Share any confidential or sensitive information of RP with any Internet site unless authorized by Superior / Management

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

1.10 Email Usage

- Email is a business communication tool and users must use this tool in a responsible, effective and lawful manner.
- RP has the authority to intercept or disclose or assist in intercepting or disclosing email communications.
- Users should use email account provided by the institution for official information.
- Confidential information will be secured before sending through e-mail by way of compression, password protection
- RP employees should treat electronic-mail messages with sensitive or confidential information
- Users shall avoid opening mail from unknown users/sources

1.11 Laptop Security

- Laptop users should take additional responsibility for the security of their laptop
- Ensure that laptop is configured as per the secure configuration.
- All sensitive data on laptop should be secured either through password protection or by using encryption.
- Whenever connecting to the LAN, ensure that updated anti-virus agent is installed
- Log off laptops when not working for extended period and enable screen
- 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.
- Loss of laptop should be reported immediately to Admin Dept / ICT Dept.

CHAPTER 2: ASSET MANAGEMENT POLICY

2.1 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

- 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 owner shall note in the asset inventory all the critical information assets required to be recovered in a disaster.

2.2 Ownership of assets

"All RP 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.
-

2.3 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.
- 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

CHAPTER 3: PERSONNEL SECURITY POLICY

The objective of this policy is to ensure that employees of RP 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 during employment.

P O Box 164, Kigali
Address: KK 15 Road, Kigali
Website: www.rp.ac.rw
Email: info@rp.ac.rw

3.1. During employment

- Appropriate awareness trainings and regular updates on organizational policies and procedures will be provided to all RP employees.
- All RP employees, Contractors and Third party users are required to follow the information security policies and procedures.

3.2. 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. 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.
- HR department will ensure that all the assets of the organization e.g. Service ID cards, laptops are returned by the outgoing employee.

CHAPTER 4: PHYSICAL AND ENVIRONMENTAL SECURITY POLICY

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

The practices of “clear desk” and “clear screen” should be encouraged to reduce the risk of unauthorized opportunist access to facilities.

4.1. 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,

4.2 Environmental Security

- The backup files and sensitive paper documents will be kept securely off-site.
- specifications taking into account air conditioning, humidity etc.
- Fire detection and suppression systems will be installed to safeguard Institution assets against fire.

- RP 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 organizational physical security systems should be properly managed by both Admin department and ICT department to effectively and securely operate them.

CHAPTER 5: COMMUNICATION AND OPERATIONS MANAGEMENT POLICY

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

5.1. Operational procedures and responsibilities

Documented Operating Procedures

- Operating procedures for information systems will be documented and authorized by the management. 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.

Change Management

- Formal management responsibilities and procedures shall be in place to ensure satisfactory control of all changes to equipment.
- A Change Management Log must contain, but is not limited to:

  - Date of submission and date of change
  - Owner and custodian contact information
  - Nature of the change

5.2. Protection against Malicious and Mobile Code

Controls against malicious code

- 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 Support team shall ensure that the updated anti-virus software is running.
- The IT Support team shall ensure that users log into their desktops using "normal user" privileges.
- All emails messages shall be scanned before entering and leaving the organization.
- All users shall be trained on the best practices to be followed while using computer systems

5.3. Back-up

Information backup and archival

- The ICT Unit shall maintain a record of all data that needs to be backed up
- 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
- 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.

5.4. 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."

Security of Network Services

- The ICT Director shall ensure that sufficient technology controls are implemented whilst taking security/network services from a 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.

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…..

5.5. 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

- RP 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

5.6. Exchange of information

Information Exchange Policies and Guidelines

- Sensitive information will be protected using encryption, password or any other suitable method especially when being sent as an attachment in an email.
- 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.

CHAPTER 7: ACCESS CONTROL POLICY

Access to RP 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. 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.

7.2. User authentication for external connections

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

7.3. 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 RP networks shall be identified and monitored

7.4. 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.

7.5. 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.

7.6. 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.

7.7. 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.

7.8. 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.

7.9. 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.
- Users shall reasonably ensure mobile devices are physically secure at all times if they contain Institution sensitive data.
- 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 a mobile device contains sensitive Institution data, it shall be encrypted on the storage drive.
  - Users are strongly encouraged to back up their Institution data stored on mobile devices.
- Remote connections to the RP network shall be made from mobile devices at public places only after obtaining prior approval from the respective unit and Infrastructure Owner.
  - Users must use an approved personal firewall, and have it running and actively filtering traffic, when connecting to RP 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. The plan must be maintained current and tested / exercised regularly.

P O Box 164, Kigali
Address: KK 15 Road, Kigali
Website: www.rp.ac.rw
Email: info@rp.ac.rw

- 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.