National Cyber
Security Authority

Minimum Cybersecurity Standards for Public Institutions

July 2023

Document Title: Minimum Cybersecurity Standards for Public Institutions

Document History:

Publication Date	Version No.	Description
28 July 2023	1.0	First release

CONTENTS

LIST of TABLES

1 Foreword

The National Cyber Security Authority issued this standard as the implementation of the responsibilities and authority indicated in article 9 point 3 and article 10 point 1 of Law No 26/2017 of 31/05/2017 establishing the National Cyber Security Authority and determining its mission, organisation and functioning.

This standard was developed in order to specify the minimum cybersecurity requirements for public institutions to ensure confidentiality, integrity and availability of their networks, business processes, customers' and stakeholders' data, as well as public sector institutions' mission critical infrastructure and ICT systems in Rwanda. Compliance with these requirements is necessary to minimize the risk of functional disruption of public institutions.

Public institutions should comply with this standard's requirements within 1 year from its publication date.

This standard should be reviewed at least every 4 years.

2 Introduction

These minimum cybersecurity standards consist of baseline cybersecurity requirements, guidelines and practice to implement in Rwanda's public institutions.

Each chapter from 4 to 21 describes one security control family.

This standard contains requirements on 2 levels of the public institutions' cybersecurity maturity – *basic* and *enhanced*. Selection and implementation of *basic* or *enhanced requirements* shall depend on the size and nature of the institution and risks identified during the risk assessment.

- **Basic** is the set of basic cybersecurity requirements to be implemented by all public institutions.

- **Enhanced** is the set of advanced cybersecurity requirements for public institutions processing critical information/data and/or operating critical information infrastructure, which could lead to a significant disruptive effect on its availability and/or integrity or have a severe impact on social and economic factors of the nation, should it fail.

The method of implementing specific requirements is influenced by the following:

1. the nature of the organization,
2. the processes implemented in it as well as its size and structure, which determine the saturation with ICT systems,
3. the development of own competences in the field of information technologies, including cybersecurity,
4. organization's readiness to use the services of external entities.

It is necessary to remember that all these factors will change over time.

Note 1: Public institution can waive those requirements which are impossible to implement in the given conditions (technically or organizationally) or, following the risk assessment, do not apply to it, or the objective specified in the requirement is ensured using other security measures. Waive of meeting a specific requirement should be justified, documented and approved by the entity's top management and communicated to NCSA accordingly.

Note 2: The order in which the requirements are presented in this document does not reflect their importance nor imply the order in which they should be implemented. List items are numbered only for ease of use and reference.

Note 3: The requirements contained in this document apply only to public institutions located within the territory of the Republic of Rwanda.

Note 4: This standard concerns infrastructure (network devices, hosts and endpoints etc.), software, services and data in possession of the public institution.

Note 5: It is recommended and encouraged for public institutions not to limit implementation controls to the basic security requirements but to implement the highest possible level of security measures which will help enhance their resilience.

3 Terms, definitions and abbreviated terms.

3.1 Terms and definitions

Term	Definition
Access control	Means to ensure that access to assets is authorized and restricted based on business and security requirements.
Accountability	Responsibility of an entity for its actions and decisions.
Asset	Anything that has value to the institution. Note: There are many types of assets, including: a) information; b) software, such as a computer program; c) physical, such as a computer; d) services; e) people and their qualifications, skills, and experience; and f) intangibles, such as reputation and image.
Authentication	Provision of assurance that a claimed characteristic of an entity is correct.
Authenticity	Property that an entity is what it claims to be.
Availability	Property of being accessible and usable upon demand by an authorized entity.
Baseline security	The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity and/or availability protection.
Business continuity	Processes and/or procedures for ensuring continued business operations.
Chief Information security officer	Person responsible in the institution for information security and cybersecurity management.
Computer Security Incident Response Team	A computer security incident response team, or CSIRT, is a group of ICT professionals that provides an organization with services and support surrounding the assessment, management and prevention of cybersecurity-related emergencies, as well as coordination of incident response efforts.
Communication infrastructure	Part of ICT infrastructure used for data transmission in public networks (WAN, Internet).
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Control Countermeasure Security control Security measures Safeguard	Means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.
Cybersecurity	1. The process of protecting information by preventing, detecting, and responding to attacks. 2. The protection of global domain consists of interdependent information and communication technology infrastructure networks.
DomainKeys Identified Mail	An email authentication method that helps prevent spoofing and phishing attacks by verifying the sender's identity and the integrity of the message. DKIM works by adding a digital signature to the email header, which can be checked by the recipient's email server using a public key published in the sender's domain DNS records.
Guidelines	Recommendation of what is expected to be done to achieve an objective.
Information asset	Knowledge or data that has value to the institution.
Information security	1. Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability, can also be involved. 2. The practice of protecting information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.
Information security incident Security incident	1. Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. 2. Any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an Information System or information stored on such Information System.
Information security event	1. Identified occurrence of a system, service or network state indicating a possible breach of information security, policy or failure of controls, or a previously unknown situation that can be security relevant.

	2. Cybersecurity event – A cybersecurity change that may impact organizational operations (including mission, capabilities, or reputation).
Information Security Management System	ISMS provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving the protection of information assets to achieve business objectives based upon a risk assessment and the organization's risk acceptance levels designed to treat and manage risks effectively. ISMS consists of policies, processes, procedures, organizational structures, software and hardware to protect the identified information assets.
Information Security Policy	1. overall intention, direction, security rules, and requirements formally expressed by top management to ensure the preservation of confidentiality, integrity and availability of information. 2. aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
Infrastructure ICT infrastructure	A discrete set of electronic information resources with system firmware/software like servers, disk arrays, network devices, communication devices, user workstations, mobile devices, and computer peripherals (printers, tape libraries etc.).
Infrastructure as code	The process of managing and provisioning an organization’s IT infrastructure using machine-readable configuration files rather than employing physical hardware configuration or interactive configuration tools.
Integrity	Property of accuracy and completeness.
Media	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Mobile Device	A portable computing device that: (i) has a small form factor such that a single individual can easily carry it; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable data storage; and (iv) is powered-on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.

	Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device. In this standard, a laptop (notebook) is considered as a mobile device.
Network	Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centres, and technical control devices.
Non-repudiation	Ability to prove the occurrence of a claimed event or action and its originating entities.
Non-privileged account	An information system account with approved authorizations of a non-privileged user (ordinary user, operator etc.) that is not authorized (and therefore, trusted) to perform security-relevant functions.
Privileged account	An information system account with approved authorizations of a privileged user (administrator, security officer) that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Procedure	Specified way to carry out an activity or a *process.*
Process	Set of interrelated or interacting activities which transforms inputs into outputs.
Public institution	An agency is established by a law, an order or through a competent authority's decision.
Reliability	Property of consistent intended behaviour and results.
Risk	Effect of uncertainty on objectives. Note 1: An effect is a deviation from the expected — positive or negative. Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood. Note 3: Risk is often characterized by reference to potential “events” and “consequences” or a combination of these. Note 4: Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated “likelihood” of occurrence. Note 5: In the context of information security management systems, information security risks can be expressed as the effect of uncertainty on information security objectives. Note 6: Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.

	Note 7: effect of uncertainty causes deviation – positive or negative. In the context of this document, only a negative deviation is considered.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk analysis	Process to comprehend the nature of risk and to determine the level of risk. Note 1: Risk analysis provides the basis for risk evaluation and decisions about risk treatment.
Risk evaluation	Process of comparing risk analysis results with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Note 1: Risk evaluation assists in the decision about risk treatment.
Risk identification	Process of finding, recognizing and describing risks. Note 1: Risk identification involves the identification of risk sources, events, their causes and their potential consequences
Risk management	Coordinated activities to direct and control an organization with regard to risk.
Risk treatment	Process to modify risk. Note 1: Risk treatment can involve: • Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • Taking or increasing risk in order to pursue an opportunity; • Removing the risk source; • Changing the likelihood; • Changing the consequences; • Sharing the risk with another party or parties (including contracts and risk financing); • Retaining the risk by informed choice. Note 2: Risk treatments that deal with negative consequences are sometimes referred to as “risk mitigation”, “risk elimination”, “risk prevention”, and “risk reduction”. Note 3: Risk treatment can create new risks or modify existing risks.
Security zone	An area and its resources for which physical security requirements have been defined.
Service-Level Agreement (SLA)	A part of a service contract, where a service is formally defined. Particular aspects of the service – scope, quality, responsibilities -are agreed between the service provider and the service user.
System	A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or

Information system ICT system	disposition of electronic information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems. The system can be understood as a combination of ICT infrastructure and application software that implements services for system users.

Table 1 – Terms and definitions

3.2 Abbreviations

API	Application Programming Interface
BYOD	Bring Your Own Device
CISO	Chief Information security officer or any other staff (Head of cybersecurity department or similar accountable role etc.) in charge of information security/cybersecurity functions in the institution.
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DKIM	DomainKeys Identified Mail
DMZ	Demilitarized Zone
DNS	Domain Name System
ICT	Information and Communications Technology
IDE	Integrated Development Environments
IPS/IDS	Intrusion Prevention System/Intrusion Detection System
ISMS	Information Security Management System
ISP	Information Security Policy
ISMS	Information Security Management System
LAN	Local Area Network
LLMNR	Link-Local Multicast Name Resolution
MFA	Multifactor Authentication
NAC	Network Access Control
NGFW	New Generation Firewall
NPI	Nonpublic Information

	Note 1: Categories of data that need to be protected in government institutions are presented in ICT Implementation Guidelines for GoR, issued by Rwanda Information Society Authority, sub-chapter 5.2. Note 2: Personal data (articles 11, 37 and 38 of [Law 058/2021]) should be included in NPI.
NSC	Network security controls
PII	Personally Identifiable Information / Personal Data
RDP	Remote Desktop Protocol
RA	Risk Assessment
SIEM	Security Information and Event Management
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
WAN	Wide Area Network
WAF	Web Application Firewall
WPAD	Web Proxy Auto-Discovery Protocol

Table 2 – Abbreviations

4 Security Policy and procedures

4.1 Basic Security Requirements

4-1. The public institution has, as a minimum, a documented Information Security Policy (ISP) based on information security requirements defined in this document and applicable legal, statutory and regulatory requirements.

4-2. Information security and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and interested parties, and reviewed at planned intervals and if significant changes occur.

PRACTICE

ISP and procedures should be reviewed at least once a year or if significant changes occur*. The review should be conducted with the participation and commitment of the management.*

4-3. The institution can create topic-specific policies, extending and supplementing the ISP related to chapters of this standard.

4-4. The institution has documented operating procedures for information processing facilities. Operating procedures must be available to personnel who need them. Operating procedures are reviewed at planned intervals, and if significant changes occur.

PRACTICE 1

ISP and procedures should be reviewed at least once a year.

PRACTICE 2

1. *Operational procedures should include at least:*
   a) *instructions for installing, configuring and updating systems and software,*
   b) *rules for recording, monitoring and handling errors or exceptions, including restrictions on the use of system tools,*
   c) *rebooting and restoring the system in case of failure (at least one per year), ISP compliance with this standard and other legal regulations should be checked.*
2. *Internal audits should be carried out following the best practices in this area*[1] *.*
3. *The internal audit may be carried out by the employees of public institutions with appropriate training or approved third parties.*
4. *The institution should document and keep all the reports from occurred internal and external audits.*

4.2 Enhanced Security Requirements

4-5. The institution develops, documents, periodically (at least once per year or when needed) updates, and implements security plans for organizational information systems.

4-6. Security plans should describe the controls in place (or planned) for the information systems and the rules of behaviour for individuals accessing the information systems.

[1] e.g. in ISO 19011 - annual audit program, audit plans, auditing techniques, codes of conduct for auditors, audit reports with conclusions, non-conformities and opportunities for improvement, etc.

4-7. If the public institution's activity is critical to the state, national security, and public safety or if it processes large amounts of critical NPI, then the public institution is recommended to implement and certify ISMS.

PRACTICE

To implement ISMS, the public institution has to use ISO/IEC 27001 [ISO27001] international standard.

5 Access Control

5.1 Basic Security Requirements

5-1. The institution limits system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).

5-2. The institution limits system access to the types of transactions and functions that authorized users are permitted to execute (role-based access control).

PRACTICES

1. *The institution should:*
   - a) *implement procedures for granting, amending, withdrawing and registering user authorizations and their periodic verification;*
   - b) *have up-to-date documentation on which systems the user has access to;*
   - c) *revoke or change entitlements immediately after the occurrence of circumstances such as, for example, a change of position or termination of employment (revoking or changing entitlements may also be an item on the employee's turnover card);*
   - d) *assign authorization tasks to competent personnel.*
2. *in the case of revoking authorizations, persons responsible for granting access (physical and ICT) should:*
   - *review the permissions related to the withdrawn account;*
   - *block access rights to ICT systems, including deactivating identifiers, access cards, ID cards, subscriptions, changing or deactivating passwords, VPN, etc.;*
   - *change access codes for doors, deposit boxes, etc.*
3. *Users must be given unique IDs;*
4. *The use of unique identifiers by a given user is aimed at establishing a relationship between a given user and specific activities in the ICT system and assigning responsibility for them;*
5. *Procedures should also include periodic checking and deletion or blocking of unused (redundant) identifiers;*
6. *Identifiers should be used once, i.e., an identifier once used should not be assigned again;*
7. *The use of group identifiers should be allowed (and documented) only in justified cases and should be supported by other accountability mechanisms, e.g., a paper duty roster;*
8. *Assigning unique identifiers to users should also apply to users from outside the organization, e.g., contractors, suppliers, integrators, etc. Such identifiers should have an expiry date, e.g., for the contract duration with a given contractor, supplier, or integrator*.
9. *Users with the need for access to the ICT systems will require authorization. Access should be granted only after the access request is approved.*
10. *For cases where roles and/or responsibilities have changed, or the users have left the institution, the access will be revoked immediately*.

11. Number of unsuccessful logon attempts should depend on the system/application and is defined by the public institution. Using values from 3 (privileged accounts) to 5 or 7 (other accounts) is recommended.

5-3. The organization should have a procedure for removal of access rights (termination) for all departing or resigning personnel, both employees and contractors/third parties. This procedure should coordinate management decision with the system administrator/personnel who is responsible for executing system access termination.

5-4. In case of malicious activity done by the employee, or contractor (third-party employee), access rights should be immediately revoked according to the incident response procedure.

5.2 Enhanced Security Requirements

5-5. The institution monitors the flow of NPI following approved authorizations.

5-6. The institution separates the duties of individuals to reduce the risk of malevolent activity without collusion.

5-7. The institution uses the principle of least privilege, including specific security functions and privileged accounts.

5-8. The institution uses non-privileged accounts or roles when accessing non-security functions.

5-9. The institution prevents non-privileged users from executing privileged functions and captures the execution of such functions in audit logs.

PRACTICES to 5-7, 5-8, 5-9, 5-17, 9-5, 9-6

The institution should manage privileged access rights as follows:

1 Privileged access rights should be identified by system or process, and the users to whom they are granted should be identified. The ICT Department lead should document all privileged access rights. Particular attention should be paid to administrative rights;

2 Administrative rights to operating systems, databases and applications should be limited to the necessary minimum, depending on the tasks to be performed;

3 Permissions granted to privileged employees (administrators) can be divided, for example, into three different accounts:

a) regular user account;

b) work on servers account - ss_name.surname ;

c) local admin account - dd_name.surname ;

4 Administrative rights should be regularly (at least once a year) reviewed and verified, e.g., by the owner of a given resource or mutually by individual administrators;

5 Access to privileged accounts should be continuously monitored using appropriate tools (e.g., SIEM, PAM, EDR, etc.).

6. To ensure proper security practices, privileged accounts should not be used for unrelated business activities. For instance, administrators should utilize regular user accounts when engaging in general tasks such as browsing the internet, checking emails, or performing office-related activities. They should reserve privileged accounts solely for critical activities that require elevated access, such as server administration, system maintenance, or network configuration changes. This segregation of privileged

and non-privileged tasks helps minimize security risks and potential unauthorized access to sensitive systems;

7 Multi-factor authentication should be used for all privileged accounts while accessing critical systems, when applicable. Access to privileged accounts should be prohibited if remote and MFA is not applicable (see Table 3*, Chap. 9).*

8 It is recommended to implement Privileged Access Manager solution for remote maintenance access to ICT infrastructure, particularly when access is performed by an external service provider (technology provider, application developer, etc.).

5-10. The institution limits unsuccessful logon attempts.

5-11. The institution provides privacy and security notices consistent with applicable NPI rules.

5-12. The institution's computer workstations have session lock enabled to prevent access and viewing of data after a period of inactivity.

5-13. The institution terminates (automatically) a user session after a defined condition.

5-14. The institution monitors and controls all internal and remote access sessions.

5-15. The institution uses cryptographic mechanisms to protect the confidentiality of remote access sessions.

5-16. The institution routes remote access via managed access control points.

5-17. The institution authorizes remote execution of privileged commands and remote access to security-relevant information.

5-18. The institution authorizes wireless access prior to allowing such connections.

5-19. The institution protects wireless access using authentication and encryption.

5-20. The institution controls the connection of corporate endpoints or mobile devices.

5-21. The institution encrypts NPI on mobile devices and mobile computing platforms.

PRACTICES to 5-20, 5-21

1 Procedures and mechanisms for securing own mobile devices outside the institution's premises should include at least:

- *requirements for physical protection of devices,*
- *software installation restrictions,*
- *rules of protection against unauthorized access,*
- *rules for using Internet services and applications,*
- *rules of conduct in the event of loss or damage to the device,*
- *mechanisms for effectively protecting mobile device communication with the institution's LAN network and internal systems.*

5-22. The institution verifies and controls/limits connections to and use of external systems.

5-23. The institution limits the use of portable storage devices.

5-24. The institution controls NPI posted or processed on publicly accessible systems.

PRACTICE 4

The institution should control the connection of mobile devices or other end-points in the following ways:

1. *Establish a mobile device policy. The policy should cover topics such as which devices are allowed to connect to the network, which types of data can be accessed on mobile devices, and how devices should be secured.*
2. *Use mobile device management (MDM) software. MDM software can be used to manage and control the connection of mobile devices to the institution network. MDM software allows administrators to remotely monitor and manage devices, set security policies, and enforce compliance with the organization's mobile device policy.*
3. *Implement network access control (NAC) system: Network access control can be implemented to ensure that only authorized devices are able to connect to the organization's network. This can include requiring users to enter a username and password or using other authentication methods such as biometrics or other multi-factor authentication methods*.

See also practices to Chapter 17 related to Access Control.

6 Awareness and Training

6.1 Basic Security Requirements

6-1. The institution ensures that executives, senior management, managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

6-2. The institution ensures personnel are trained to carry out their assigned cybersecurity related duties and responsibilities.

PRACTICES

1. *Awareness and training processes should be considered in the following 2 areas:*

   b) *Cybersecurity awareness,*

   c) *Professional education and training*

2. *Initial awareness, education and training can apply to new personnel and those who transfer to new positions or roles with substantially different information security requirements. Personnel's understanding should be assessed at the end of an awareness, education or training activity to test knowledge transfer and the effectiveness of the awareness, education and training program.*

3. *A cybersecurity awareness program should aim to make personnel aware of their cybersecurity responsibilities and the means by which those responsibilities are discharged.*

4. *The awareness program should be planned considering the roles of personnel in the organization, including internal and external personnel (e.g., external consultants, and supplier personnel) and should include the best practices in information security and cyber security.*

5. *The activities in the awareness program should be scheduled over time, preferably regularly (at least twice a year). It should also be built on lessons learnt from occurred cybersecurity incidents.*

6. *The awareness program should include several awareness-raising activities via appropriate physical or virtual channels such as campaigns, booklets, posters, newsletters, websites, information sessions, briefings, e-learning modules and e-mails.*

7 *The organization should identify, prepare and implement an appropriate training plan for technical teams whose roles require specific skill sets and expertise. The education and training program should consider different forms, for example:*

   - *lectures or self-studies, being mentored by expert staff or consultants,*
   - *rotating staff members to follow different activities,*
   - *recruiting already skilled people,*
   - *and hiring consultants.*

8 *The institution should have a mechanism in place to evaluate the effectiveness of the awareness session.*

9 *The management should have a cybersecurity awareness program extended according to the position held (e.g., supervision of employees, specific roles and responsibilities, etc.).*

6.2 Enhanced Security Requirements

6-3. The institution provides security awareness training on recognizing and reporting potential indicators of insider threat.

PRACTICE 1

The good way to perform security awareness training is to present real examples of attacks (phishing, ransomware infection, etc.) and their impact on the user and his/her institution.

PRACTICE 2

Various tests and metrics can be used to verify the effectiveness of information security (cybersecurity) training and awareness campaigns, for example:

1. *Basic approach - percentage of employees who participated in the training/campaign (an indicator of 70% during the year can be considered as satisfactory, 90% as good and 100% as very good) – percentage can be changed by the institution;*
2. *Advanced approach - the percentage of employees who answered positively to 70% of the questions in the knowledge test regarding the scope of the above. training/campaign – the percentage of employees can be changed by the institution;*
3. *Active - social engineering tests - e.g., phishing campaign: sending an e-mail to employees with an attachment in the form of a file or link and assessing their reaction (ignoring the email/launching / notification of the information security event). The attachment can be suspicious (e.g., exe file, Office document with a macro, etc.), but not contain any real malware.*

7 Audit and Accountability

7.1 Basic Security Requirements

7-1. The institution creates and retains system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.

7-2. The institution ensures that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.

PRACTICES to 7-1, 7-2

Audit logs and records should meet the following requirements:

1 An event logging system in networks and ICT systems should be implemented and procedures for archiving the collected logs should be developed. Logs should be retained for at least 12 months.

2 The event log should contain at least information about:

- *user ID,*
- *date, time and details of important events, e.g., starting and ending work in the system, including failed login attempts,*
- *changes in system configuration,*
- *use of privileges,*
- *changes to privileges,*
- *use of selected system tools and applications,*
- *network addresses,*
- *alarms raised by the access control system,*
- *activation and deactivation of protection systems, e.g., anti-virus software.*

3 ICT system administrators should not be authorized to delete or deactivate logs containing records of their own activities, and for systems where this is impossible, a mechanism for copying to an external repository - log servers or SIEM systems should be provided.

7.2 Enhanced Security Requirements

7-3. The institution reviews, and updates logged events.

7-4. The institution alerts in the event of an audit logging process failure.

7-5. The institution correlates audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.

PRACTICES to 7-3, 7-4, 7-5, 7-8

1 SIEM tools or equivalent service can store, correlate, normalize and analyze log information, and generate alerts. SIEMs tend to require careful configuration to optimize their benefits. Configurations to consider include identifying and selecting appropriate log sources, tuning and testing rules, and developing use cases.

2 SIEM tools typically protect the integrity and confidentiality of stored audit logs.

7-6. The institution provides audit record reduction and report generation to support on-demand analysis and reporting.

7-7. The institution provides a system capability that compares and synchronizes internal system clocks with an authoritative source (NTP servers) to generate time stamps for audit records.

PRACTICE

The time source can be the time servers of pool.ntp.org.

7-8. The institution protects audit information and audit logging tools from unauthorized access, modification, and deletion.

7-9. The institution limits management of audit logging functionality to a subset of privileged users.

8 Configuration Management

8.1 Basic Security Requirements

8-1. The institution establishes and maintains baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles. The inventory should contain information about all users and all accounts in systems and applications.

PRACTICE

The inventory of IT resources and their configuration should contain information relevant to the proper functioning of a given resource, such as passwords, configuration data, cryptographic keys, etc.

8-2. The institution establishes and enforces security configuration settings for information technology products employed in organizational systems.

8.2 Enhanced Security Requirements

8-3. The institution tracks, reviews, approves or disapproves, and logs configuration changes to the organizational systems.

8-4. The institution analyzes the security impact of changes prior to implementation.

8-5. The institution defines documents, approves, and enforces physical and logical access restrictions associated with changes to organizational systems. In particular:

a) development, testing and production environments shall be separated and secured;

b) before a change in the configuration is introduced to the production environment, a change request should be approved by a competent department or person in charge. Depending on the type or nature of the change, ICT and/or security departments should approve the request and/or be informed of the request.

PRACTICES to 8-5

If the institution uses development, test and production environments, it should follow the following recommendations:

1 The institution should define and document the rules for transferring software from the development level to the production level;

2 Changes to production systems and applications, if possible, should be tested in test or pre-production environments before their implementation;

3 Access of development and testing personnel to the production environment should be limited to the minimum necessary;

4 In test and development environments, real data from the production environment (e.g., copied) should be limited to the necessary minimum and only if the test environment is secure;

5 If information relevant to the security of the ICT infrastructure is available in test and development environments (e.g., access data, configuration details security), they should be secured analogously to the production environment;

6 If the test and development environments are not to (will not) be used any longer, the data collected on them should be securely deleted. This process should be documented.

8-6. The institution uses the principle of least functionality by configuring organizational systems to provide only necessary capabilities.

PRACTICES to 8-5, 8-6, 8-9

1 Procedures for the supervision of software installation in a production environment should include at least:

- *rules for updating production software, applications and libraries;*
- *allowing only approved and tested executable code into production systems (no compilers or code under development should be allowed);*
- *rules for restoring the previous version of the system, including the preservation of previous versions of the software.*

8-7. The institution restricts, disables, or prevents the use of unnecessary or dangerous programs, functions, ports, protocols, and services.

8-8. The institution applies deny-by-exception (blacklisting) policy to prevent the use of unauthorized software or deny-all (permit-by-exception) policy to allow the execution of authorized software.

8-9. The institution controls and monitors user-installed software.

PRACTICES to 8-9

The institution should have implemented policies and mechanisms for installing software by users, as follows:

1 Prevent users from installing software. Authorizations to install software allowed (specified) by the operator should be granted only to appropriate administrators;

2 Web browsers should be configured to block the automatic launch of malicious scripts on websites and unused or discontinued plug-ins (e.g., Flash, Java, Silverlight). Disable all unused features of Microsoft Office software, web browsers and PDF readers;

3 Have a list of allowed software on users' workstations. This list should be used by a service desk configuring these workstations. Management must approve changes to the above list and exclusions for specific users (roles).

4 Reviews of installed software in the institution's networks and ICT systems should be carried out, and mechanisms should be implemented at least once a year for periodic compliance checks of the software installed with the list of software approved for use in the network.

9 Identity Management and Authentication

9.1 Basic Security Requirements

9-1. The institution identifies system users, processes acting on behalf of users, and devices.

9-2. The institution authenticates (or verifies) the identities of users, processes, or devices as a prerequisite to allowing access to organizational systems.

9-3. The institution enforces a minimum password complexity and change of characters when new passwords are created.

9-4. The institution allows temporary password use for system logons with an immediate change to a permanent password.

9.2 Enhanced Security Requirements

9-5. The institution uses multifactor authentication for local and remote (network) access to privileged accounts and to non-privileged accounts, according to Table 3.

	High criticality/sensitivity system		Medium/Low criticality/sensitivity system	
	Local access (LAN)	Remote access (WAN/Internet)	Local access (LAN)	Remote access (WAN/Internet)
Privileged account	MFA Mandatory	MFA Mandatory	MFA Mandatory	MFA Mandatory
Non-privileged account	MFA Mandatory when applicable	MFA Mandatory when applicable	MFA Optional (follow Risk Assessment results)	MFA Optional (follow Risk Assessment results)

Table 3 – Conditions for using MFA to access information systems

9-6. The institution uses replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.

9-7. The institution prevents the reuse of identifiers for a defined period.

9-8. The institution disables identifiers after a limited period of inactivity.

9-9. The institution prohibits password reuse for a specified number of generations.

9-10. The institution stores and transmits only cryptographically-protected passwords.

9-11. The institution obscures feedback on authentication information.

PRACTICES

1 The institution should have procedure(s) for transferring and storing user authentication data, ensuring the confidentiality of this data. Procedure(s) should take into account the following:

- *confidential credentials may include, for example passwords, cryptographic keys, data stored in hardware tokens;*
- *in the case of temporary/default passwords assigned to the user, their uniqueness should be ensured, and the need to change them upon first use should be enforced;*
- *Keep password hashes only; if you need to retrieve it, keep it in a secure environment, such as a vault or safe.*

2 *The institution should have procedure(s) for secure logging into ICT systems responsible for supporting critical processes carried out by it. Procedure(s) should take into account the following:*

- *The method of authentication should be adapted to the nature of a specific system and the data processed in it, as well as to the assessment of the effects of the risk of unauthorized access;*
- *All remote access sessions should be automatically logged. This applies to both employees and service providers (e.g., external technical personnel);*
- *In the case of remote access, solutions should be used to encrypt data transmission, such as VPN, SSH or other, preventing eavesdropping and interception of information;*
- *In ICT systems responsible for supporting critical processes carried out by the institution, multi-factor authentication should be used.*

3 *The institution should have password management procedure(s), that take into account the following:*

- *A policy of constructing "strong" passwords and forcing them to be changed in the event of suspicion of compromise or in administrative mode (by the administrator) should be introduced;*
- *The use of local administrative accounts should be blocked;*
- *The use of local administrative accounts built into some operating systems should be blocked;*
- *Password managers or hardware-encrypted flash drives can also be used in the case of systems (network devices) that cannot be covered by directory services, TACACS, RADIUS, and in particular, in the event of loss of communication with these systems.*

4 *The institution should regularly review access logs of privileged accounts and document the results to identify any possible account abnormal behaviours.*

5 *The institution should consider to implement MFA to access all accounts in the organizational ICT systems, particularly for remote access via the public network taking into account risk assessment results (according to Table 3).*

10 Incident Response

10.1 Basic Security Requirements

10-1. The institution has an operational incident-handling capability for organizational systems, including preparation, detection, analysis, containment, recovery, and user response activities.

10-2. The institution must notify the public authority in charge of cybersecurity about every incident. This also pertains to the incidents that can be handled by the institution itself. If the institution cannot handle the incident and/or the incident concerns critical public safety, the institution should request support from the appropriate public authority.

PRACTICE 1

The Rw-CSIRT (Rwanda Computer Security Incident Response Team) can provide incident prevention and response services for public institutions when requested or notified by the affected institution. The Rw-CSIRT should be notified on every cyber incident that is likely to significantly impact public health or safety, the provision of wide-scale critical infrastructure services, socio-economic stability or national security. The catalogue of services provided by Rw-CSIRT can be found in RFC2350 (Available on https://cert.gov.rw/)

PRACTICE 2

The institution should have mechanisms in place to enable immediate reporting of events related to cybersecurity. In addition to automated systems, the institution's staff is the basic source of information about events related to cybersecurity, therefore, they should be trained in this area.

10-3. The institution has documented and implemented procedures for responding to cybersecurity incidents. The procedures should include at least:

- reporting information security incidents,
- planning and preparing to respond to incidents,
- monitoring, detecting, analyzing and reporting events and incidents related to information security,
- response, including escalation, supervised post-incident recovery and internal and external communications.

10-4. The public institution ensures that incident-handling capability is supported at the appropriate level by human, technical, information and financial resources.

PRACTICE 1

Competent staff is the most important element of incident response.

PRACTICE 2

The number of events requiring constant analysis in terms of security may impose the use of advanced ICT systems supporting the process of detecting security breaches;

10-5. The institution tracks, documents, and reports incidents to designated officials or authorities internal and external (see 10-2).

PRACTICE 1

Establishing and maintaining operational contacts channels with relevant authorities, bodies and services is necessary, especially with Rw-CSIRT.

PRACTICE 2

Participate in the exchange of information on incidents and vulnerabilities with other institutions.

10.2 Enhanced Security Requirements

10-6. The institution tests the institutional incident response capability.

10-7. The institution collects and analyzes information relating to cybersecurity threats to produce cyber threat intelligence.

PRACTICE 3

The best method to produce CTI is to use existing feeds, for example, from own CTI team or other teams, services and sources in the following ways:

a) Receive system security alerts, advisories, and directives on an ongoing basis;

b) Generate internal security alerts, advisories, and directives as deemed necessary;

c) Disseminate security alerts, advisories, and directives to personnel or roles defined in the Information Security Policy;

d) Implement security directives following established time frames, or notify the issuing organization of the degree of noncompliance;

e) Where applicable, CTI feeds provided by Rw-CSIRT should be taken into consideration.

11 Maintenance

11.1 Basic Security Requirements

11-1. The institution should perform maintenance on organizational ICT systems.

11-2. The institution provides controls on the tools, techniques, mechanisms and personnel used to conduct system maintenance.

11.2 Enhanced Security Requirements

11-3. The institution ensures equipment removed for off-site maintenance is sanitized of any NPI.

11-4. The institution checks media containing diagnostic and test programs for malicious code before the media are used in organizational systems.

11-5. The institution requires multifactor authentication, according to Table 3, to establish nonlocal maintenance sessions via external network connections and terminate such connections when nonlocal maintenance is complete.

11-6. The institution must organize and supervise the maintenance activities of maintenance personnel, which are usually performed without required access authorization, except those who are pre-authorized to perform.

11-7. The institution applies the rules of secure design, development and modification of software and systems.

PRACTICES

Rules of secure design, development and modification of software and systems include:

a) Information security should be integrated into project management;

b) Rules for the secure development of software and systems should be established and applied;

c) Information security requirements should be identified, specified and approved when developing or acquiring applications;

d) Principles for engineering secure systems should be established, documented, maintained and applied to any information system development activities;

e) Secure coding principles should be applied to software development (for details, see Appendix 2 – Secure application coding principles);

f) Security testing processes should be defined and implemented in the development life cycle;

g) The organization should direct, monitor and review the activities related to outsourced system development;

h) Development, testing and production environments should be separated and secured;

i) Changes to information processing facilities and information systems should be subject to change management procedures.

12 Media Protection

12.1 Basic Security Requirements

12-1. The institution protects (i.e., physically control and securely store) system media containing paper and digital NPI.

PRACTICES

An important aspect of media protection after termination of employment is the return of all resources (system media containing NPI) that have been transferred to the employee, as follows:

1 The return should cover all ICT devices issued, including, e.g., one-time code generators;

2 The return of resources should also occur in the event of a job change in a situation where the employee ceases to use a given resource as part of the performance of official duties.

12-2. The institution limits access to NPI on system media to authorized users.

12-3. The institution sanitizes or destroys system media containing NPI before disposal or release for reuse.

PRACTICES

The institution should have procedures for dealing with data carriers and ICT equipment withdrawn from current use, as follows:

1 Implement the categorization of data carriers (e.g., portable and non-portable), and then define the rules of conduct for each category;

2 Procedures should address the issuance, withdrawal and transfer of media;

3 It should be ensured that data carriers permanently leaving the organization (e.g., by way of sale, transfer or after their use) are unable to read data, e.g., by overwriting data, destroying the carrier, etc.;

4 *Using physical destruction methods, such as shredding, incineration, or degaussing, for paper-based and non-reusable digital media.*

5 Documenting the media sanitization and disposal process, including the date, media type, and personnel responsible.

6 Procedures should include blocking unapproved CD/DVD/USB media and blocking connection to unapproved phones, tablets and Bluetooth/Wi-Fi/3G/4G/5G devices. This requirement applies in particular to ICT systems responsible for supporting critical processes carried out by the institution.

12-4. The public institution ensures identification of records and their retention period, considering legislation or regulations and community or societal expectations, if applicable. Legislation that should be considered is, e.g., Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy in Rwanda (article 52). Information systems should permit the appropriate destruction of records after that period if the institution does not need them.

12.2 Enhanced Security Requirements

12-5. The institution marks media with necessary NPI markings and distribution limitations.

12-6. The institution controls access to media containing NPI and maintains accountability for media during transport outside of controlled areas.

PRACTICE

Control and maintain accountability for media containing NPI during transport outside of controlled areas by:

a. *Implementing secure packaging and transport methods, such as tamper-evident packaging or courier services with chain-of-custody tracking;*

b. *Using encrypted communication channels when transmitting NPI electronically;*

c. *Maintaining a log of media transport activities, including the sender, recipient, date, and method of transport.*

12-7. The institution implements cryptographic mechanisms to protect the confidentiality of NPI stored on digital media during transport unless otherwise protected by alternative physical safeguards.

PRACTICE

Recommendation for strong cryptography mechanisms - See Appendix 1.

12-8. The institution controls the use of removable media on system components.

PRACTICE

Control the use of removable media on system components by:

a. *Establishing a policy that outlines the acceptable use of removable media, including types of media, devices, and circumstances under which their use is permitted.*

b. Implementing technical controls, such as endpoint security solutions, to restrict the use of unauthorized removable media on system components.

12-9. The institution prohibits the use of non-corporate portable storage devices.

12-10. The institution protects the confidentiality of backup NPI at storage locations.

13 Personnel Security

Note 1: It is important to ensure personnel security is an integral part of the risk management process in the public institution. It should be remembered that many aspects of ensuring personnel security are inextricably linked to other elements of the public institution security system, such as ensuring business continuity.

Note 2: Permissions to enter the premises of the public institution are most often granted to employees of the organization (during their employment) and employees of service providers or suppliers or guests (as a result of mutual agreements or on an ad hoc basis). Physical access to subsequent security zones and the level of access to information about facilities, devices, installations and services can be used illegally and serve to disrupt the functioning of the public institution or act to its detriment.

13.1 Basic Security Requirements

13-1. The public institution identifies (inventories) its own human resources. For each official position with access to NPI, the scope of duties and the analyzed security requirements are defined (the level of access to zones, rooms, documents, systems etc.)

PRACTICE 1

The analysis of security requirements should be closely related to risk assessment (chapter 15) and access control requirements (chapter 5).

PRACTICE 2

In every organization, there are people with critical (unique) knowledge about its functioning, experience, and "institutional memory". They are particularly valuable for the organization, and at the same time, they are potentially the greatest threat in the event of an action to the organisation's detriment. The inventory should allow for identifying key personnel for the delivery and performance of critical organization's operations and services*. For such personnel, the public institution adopts the highest security requirements. Steps should also be taken to ensure the possibility of replacement with similar qualifications and authority.*

13-2. The public institution verifies the identity of employees and job candidates based on the submitted original documents (containing names, surnames, date of birth, address and photo).

PRACTICE 1

The identity of a person consists of attributes given after birth (name, surname, date and place of birth, parents' names), individual biometric features (fingerprint, iris, hand, face, DNA biometrics) and elements of biography (education, employment history).

PRACTICE 2

Documents that are difficult to convert and counterfeit, such as a passport or ID card, should be required. Check that the competent authority issues the presented document and has a valid expiry date where applicable.

13-3. The institution screens individuals prior to hiring them as well as taking up a role related to access to sensitive information. In particular, it does so before authorizing access to ICT systems of organizations containing NPI.

13-4. The institution ensures that organizational systems containing NPI are protected during and after personnel actions such as terminations and transfers.

13-5. The institution provides basic training on information security upon commencement of employment.

13-6. The institution ensures the identification of people having access to the facilities by introducing mandatory identifiers (badges).

13-7. The institution ensures that security personnel are immediately provided with information on the denial of access for the departing employee.

13-8. The institution ensures periodic verification of physical access and authorizations for employees and external subcontractors related to position and work performed.

PRACTICE 1

At least the authorizations to:

a) access to the facility,

b) *access to particular zones - if determined,*

c) *access to ICT resources,*

d) access to legally protected information - classified information.

- *should be verified.*

PRACTICE 2

Access to restricted areas is verified at least every 6 months or when it is needed for the following reasons:

a) security incident,

b) change of security policy in the field of physical security,

c) change of legal regulations.

13-9. The public institution provides all employees with awareness training in social engineering threats. Completion of the training is documented by: the training program, its duration, the instructor and the trainee's signature.

PRACTICE

The training should inform employees of the characteristics of social engineering threats, examples of such attacks and methods of protection against negative effects.

13-10. The public institution has procedures for verifying the qualifications of candidates and employees.

PRACTICE

Verification of information contained in the presented documents includes:

a) education,

b) professional experience,

c) predispositions.

13-11. The institution ensures that people with no criminal record are employed in key positions. This is done by a job candidate submitting a Criminal Record Certificate issued by the National Public Prosecution Authority (NPPA).

13.2 Enhanced Security Requirements

13-12. Public institutions follow a public procurement law that determines what the external parties have to present. For example:

a) The Ministerial Order No 002/20/10/TC of 19/05/2020 establishing regulations on public procurement;

b) Guidelines for GoR [GOV] that give out some guidelines on how to procure hardware and software for public institutions (Chapter 11).

PRACTICE

The public institution verifies companies which provide services to it and, with particular care, undertakes and updates the organization's knowledge of the risks associated with service providers, subcontractors and external suppliers. Such verification may be possible to take place through:

a) request for references,

b) analysis of the contractor's credibility using basic open-source intelligence methods,

c) inclusion in the contract of the possibility of verifying the sobriety of all contractor's employees,

d) inclusion in the contract of the possibility of verifying the content of vehicles as well as clothing and belongings brought in and carried out by the subcontractor's employees,

e) request the presentation of identity documents each time they enter the facility,

f) obligations of employees of companies providing the service in compliance with the institution's policies and rules.

14 Physical and Environmental Protection

14.1 Basic Security Requirements

14-1. The institution divides the area it manages into security zones based on risk assessment to ensure physical security.

PRACTICE 1

Each of the zones must be designed in such a way as to eliminate the anticipated attack scenarios and where it is impossible to slow down the actions of a potential attacker as much as possible.

PRACTICE 2

*The number of security measures s*hould increase as the potential attacker approaches the zone protecting key elements of the organization's infrastructure and, as a result, discourage him or allow more time to react adequately to the threat.

14-2. The institution provides, limited by the scope of official duties, access to particular security zones. The principle of necessary access applies (need to have).

14-3. The institution limits authorised individuals' physical access to organizational systems, equipment, and the respective operating environments.

PRACTICE 1

The requirement applies to employees, contractors, suppliers, subcontractors and visitors.

PRACTICE 2

Rules for entering and leaving the security zones and moving around the protected area (facilities) can be described, for example, in specific instructions. If the institution allows separate rules for certain persons (e.g., selected services, important guests, VIPs), instructions should document exceptions.

14-4. The institution provides employees with basic physical security training.

PRACTICE

1. *Basic training should be provided to all employees of the organization.*
2. *The scope of the basic train*ing should include:
    - *Threats;*
    - *Elements that make people aware of threats and identify the basic symptoms of a crisis situation;*
    - *Presentation of security measures that are in use in the institution;*
    - *Security rules, including instructions applicable in the institution;*
    - *Presentation of security roles, powers and responsibilities;*
    - *Conduct in basic situations of a terrorist nature;*
    - *Emergency preparedness that includes emergency exits, how to carry out the evacuation, where safe places are;*
    - *First aid skills, including CPR, treating cuts and wounds, and recognizing signs of shock.*

14-5. The institution protects and monitors the physical facility and supports infrastructure for organizational systems.

14-6. The institution prevents or reduces the consequences of events originating from physical and environmental threats such as fire, flood, earthquake, explosion, civil unrest, toxic waste, environmental emissions and other forms of natural disaster or disaster caused by human beings.

PRACTICE

*P*hysical security measures can include:

a) physical security personnel,

b) physical barriers (fences, walls, doors, wickets, gates),

c) access control system, which allows identification of a person based on identification data, verification of access rights and *accountability (can be implemented as an electronic access control system),*

d) visual surveillance system,

e) alarm system, which allows alerting in case of attack and attempts of illegal entrance,

f) automatic systems able to detect fires at an early stage and send alarms or trigger fire suppression systems in order to prevent fire damage;

g) automatic systems able to detect flooding at an early stage under the floors of areas containing storage media or information processing systems;

h) air conditioning system to support appropriate temperature;

i) awareness of employees.

14-7. The institution maintains audit logs of physical access. Audit logs should be stored for a minimal 12 months period.

14-8. The institution controls and manages physical access devices (badges/keys/PIN codes/cards).

PRACTICE 1

Physical access devices should be registered and individualized, e.g., by labelling or numbering.

PRACTICE 2

*The rules for storing and issuing keys to protec*ted rooms and zones, the periodic exchange of codes, and the mode of issuing and granting cards should be defined and documented

PRACTICE 3

Badges must have security features that make it difficult to alter or counterfeit them. The personal pass must have a legible image of the holder's face enabling comparison with the holder. The holder's image may also be reflected in electronic form if the institution has an electronic access control system with the holder's image displayed on the screen of the security personnel.

PRACTICE 4

*Single-use badges may not have the holder's image. In such a situation, the badge allows entry to the premises only in combination with a secured document with a phot*o issued by a state authority.

PRACTICE 5

A single-use badge must be returned each time after leaving the protected premises to authorized physical security personnel or have technical or other security measures that preclude its use after the time set for staying in the protected premises.

PRACTICE 6

Public institution phone number or e-mail address can be put on the badge to report a lost one.

14-9. The institution enforces safeguarding measures for NPI processing at alternate work sites (e.g., Disaster recovery site).

PRACTICE 1

Physical security training should include:

a) Understanding the disaster type;

b) Emergency preparedness includes the location of emergency exits, how to carry out evacuation and the location of the safe places, and assembly points;

c) Training on how to communicate effectively during a crisis;

d) Training on how to handle fire emergency (including training on using fire extinguisher and locating the fire assembly points).

e) First aid skills, including CPR (cardiopulmonary resuscitation), treating cuts and wounds, and recognizing signs of shock;

f) *How to manage stress, cope with loss, and support others who are struggling emotionally.*

PRACTICES 2

1 Extended training should be provided to security personnel and the department responsible for security.

2 The scope of the extended training should include basic training and additionally:

- *elements that make people aware of threats and identify the basic symptoms of a crisis situation,*
- *presentation of security measures that are in use in the institution,*
- *security* rules, including instructions applicable in the institution,
- *presentation of security roles, powers and responsibilities,*
- *conduct in basic situations of a terrorist nature.*

14.2 Enhanced Security Requirements

14-10. The institution assists and monitors visitors' activities.

PRACTICE

Visitors should access the facility under the supervision of an authorized employee of the institution from the moment of entering to the moment of leaving the facility.

15 Risk Assessment

15.1 Basic Security Requirements

15-1. The institution periodically – at least once a year - assesses the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals resulting from the operation of organizational systems and the associated processing, storage, or transmission of NPI.

PRACTICES

1 Risk assessment in the context of ICT resources should be part of the overall risk management process in the institution;

2. Persons responsible for the operation/maintenance of specific ICT systems should be the source of information for risk assessment carried out by the CISO or any other staff responsible for cybersecurity;

3 The first step in assessing risk is understanding the institution and its context;

4 The institution should identify all implemented processes, assess their importance for the implementation of its tasks and identify ICT resources supporting these processes and the information processed in them;

5 The information security risk assessment process[2] can be carried out as part of the organization's overall risk management process[3]or as part of the implementation of the business continuity management system[4].

6 The result of assets' assessment should be a register of assets, which should indicate their owners and the importance of the asset to the institution.

7 Asset owner is a person designated by the management to manage the asset and has the ability to make financial commitments and take related business decisions, e.g., about access to the asset;

8 Risk assessment should take place at least once a year or when necessary, which may result from the following premises:

- *occurrence of a serious incident,*
- *receiving recommendations from competent authorities,*
- *detection of new vulnerabilities threatening the functioning of the institution,*
- *change of technologies used, change of main suppliers, etc.*

9 For cases where certain risks can't/won't be removed, the institution should have a well documented risk acceptance. ICT and Security departments should know the accepted risk(s).

[2] Based on recommendations of ISO/IEC 27005 standard [ISO27005].

[3] According to the ISO 31000 standard [ISO31000].

[4] according to the ISO 22301 standard [ISO22301].

15.2 Enhanced Security Requirements

15-2. The institution scans for vulnerabilities in organizational ICT systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

15-3. The institution remediates vulnerabilities following risk assessments.

PRACTICES to 15-2, 15-3

The institution should monitor and obtain information on technical vulnerabilities of the ICT systems used on an ongoing basis and assess the organization's exposure to them, as well as take appropriate measures to counteract the related risk(s), as follows:

1 *A register of identified ICT resources supporting critical services is a prerequisite for vulnerability management;*

2 *Critical updates and fixes (after confirming that they are free of bugs) should be introduced immediately after their publication, especially regarding the elimination of 0-day vulnerabilities;*

3 *Applications should be used in the latest legal version possible and updated on a regular basis. This applies in particular to, e.g., web browsers, Microsoft Office software, and PDF readers. From the moment of their publication (and confirmation that they are error-free), the patch/correction/update of applications responsible for supporting critical processes carried out by the operator should be installed without undue delay;*

4 *Operating systems should be used in an up-to-date, legal version and kept up-to-date along with network devices. It is not recommended to use versions that are no longer supported. From the moment of their publication (and confirmation that they are error-free), the patch/correction/update of operating systems responsible for supporting critical processes carried out by the operator should be installed without undue delay;*

5 *Managing technical vulnerabilities requires specific information, such as:*

- *software provider data,*
- *version number,*
- *system where the software is installed,*
- *the duration of technical support and licenses of the software manufacturer;*

6 *Information on vulnerabilities and threats can be obtained from computer incident response teams, e.g., Rw-CSIRT (https://cyber.gov.rw/updates/alerts/).*

16 Security Assessment

16.1 Basic Security Requirements

No requirements are identified.

16.2 Enhanced Security Requirements

16-1. The institution periodically assesses the security controls in organizational systems to determine if the controls are effective in their application.

16-2. The institution develops and implements action plans designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational ICT systems.

16-3. The institution monitors security controls on a regular basis to ensure the continued effectiveness of the controls.

16-4. The institution develops, documents, and periodically updates system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other ICT systems.

PRACTICES 1

1 The best way to perform security assessment is to carry out security audits (internal and external)[5].

2 Part of the security audit can be vulnerability assessments and penetration tests (wider described in PRACTICES 2). Those tests should include:

- *Assessing vulnerabilities in the ICT systems used,*
- *Testing the possibility of intrusion into the institution's ICT systems from the Internet and other places within the internal infrastructure (infrastructural penetration tests),*
- *Testing the security of the ICT systems and applications that can be targeted in attacks (application penetration tests),*
- *Monitoring unauthorized disclosure of internal material information regarding the institution's ICT infrastructure,*
- *Assessing employees' susceptibility to social engineering attacks.*

3 Security audits should be carried on at planned intervals at least once a year. It is recommended for institutions to create an audit program that includes several internal audits during a year.

4 Vulnerability scans and penetration tests should be carefully planned, agreed and controlled with business and ICT management to reduce:

- *the likelihood of ICT systems downtime,*
- *the organization's operations or services impact.*

The institution should ensure:

[5] Audit rules and technics can be found in [ISO19011] and [ISO17021]. International Standard [ISO27001] (all clauses and Annex A points) can be used if institution intends to implement ISMS according to this standard.

- *having current backups of data and systems,*
- *choosing the right ICT environment for testing,*
- *choosing the right test time (weekend, service break, etc.).*

PRACTICES 2

There are differences between vulnerability scans and penetration testing:

1. *Penetration testing is a form of security test where security experts simulate a hack of your systems to uncover and exploit vulnerabilities*
2. *Vulnerability scans and penetration testing (both security testing) can be divided into three categories:*
    - *White Box Security Testing: This is when the security testers receive ample information about the internal structure of the target system. They go in knowing how the code should be implemented and check whether everything is aligned.*
    - *Black Box Security Testing: In this form, the testers hardly receive any information about the system's internal structure. Their work is based on input and response. This approach is similar to how a real attacker would make their moves.*
    - *Grey Box Security Testing: The Grey Box approach combines white box and black box. While the testers do not know the code structure, they are given some crucial information like login credentials. These tests are important to determine how much damage an attacker with privileged access can cause.*

17 System and Communications Protection

17.1 Basic Security Requirements

17-1. The institution monitors, controls, and protects communications (i.e., information transmitted or received by organizational systems) at the external and key internal boundaries of organizational ICT systems.

17-2. The institution uses architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational ICT systems.

PRACTICES to 17-1, 17-2, 17-5, 17-8, 17-9 as well as 5-1, 5-2, 5-22 (Access Control domain)

The institution should oversee and manage the networks as follows:

1 *ICT solutions should be introduced (e.g., firewall, VLAN type), allowing for filtering and separation of traffic to ICT systems responsible for supporting critical processes carried out by the institution;*

2 *Direct access to the Internet from ICT systems responsible for supporting critical processes carried out by the institution should be prevented;*

3 *Web content should be filtered - access to malicious domains and IP addresses, advertisements and anonymous networks should be registered, monitored and blocked.*

4 *By default, any unnecessary and unauthorized (incoming or outgoing) network traffic should be blocked (e.g., using IPS/IDS solutions and application firewalls), including those generated by untrusted applications;*

5 *Only trusted DNS servers should be used, and detailed filtering of DNS queries should be carried out;*

6 *Network traffic to and from the institution's computers where important data is stored or which are responsible for supporting critical processes performed by the institution and traffic crossing the perimeter of the organization's network should be captured for incident detection and analysis;*

7 *The "port security" functions should be used on network switches; in the basic operation, the MAC address of the network card should be associated with the port used by the device, and in the case of more advanced solutions, the NAC (Network Access Control) technology should be used using IEEE 802.1x standard mechanisms.*

8 *Disable unused services that are not required/necessary for work on a given workstation, e.g., RDP, AutoRun, LanMan, SMB/NetBIOS, LLMNR, WPAD and protocols, e.g., DHCP, IPv6, IPX etc.*

PRACTICES to 17-1, 17-2, 17-5, as well as 5-3 (Access Control domain)

1 *The institution should separate the information service networks, users and information systems as follows:*

   a) *Division into separated network domains is one method of supervising the security of large networks. Separation can be done physically or logically. Regardless of the distribution method, the boundaries of each domain and the access requirements for each domain must be clearly defined;*

b) *Cross-domain access is possible, but controlling it with devices such as a firewall or filtering router is recommended. Attempts to connect other than defined should be monitored and analyzed;*

c) *Restrict low-trust devices (e.g. IoT and BYOD devices) and restrict network access to drives and data repositories based on function.*

2 *Network Layer L3 switches are used to separate LAN into VLANs. A Layer 3 switch can perform inter-VLAN routing at wire speed with predictable performance. Still, it may not provide the same level of security and policy control as a Next-Generation Firewall (NGFW). A NGFW can provide granular policy control and advanced security features, but it may not be able to handle high-speed traffic flows as efficiently as a Layer 3 switch. The usage of both solutions together is recommended.*

PRACTICES to 17-1, 17-5, 17-8, 17-11 as well as 5-1, 5-2, 5-3 (Access Control domain)

The institution should consider using the following electronic message protection mechanisms:

1 *Crafted e-mails (phishing, spear phishing) are the basic vector of attack on institutions, therefore user education including, among others, ways to avoid phishing e-mails (e.g., with links to log in to fake websites), weak passwords, password reuse, and unapproved removable media and devices are the primary means of institution security;*

2 *Implementing:*

- *isolation (sandboxing) of network content - blocking in case of suspicious behaviour (e.g., based on network traffic, new or modified files and other unusual changes in the system),*
- *use of categorization (whitelisting) of allowed types of attachments (including archives as well as embedded archives and password-protected archives) or prohibited attachments (blacklisting),*
- *analyzing/cleaning links, PDF files and Microsoft Office macro quarantine or configuration,*
- *using the Sender Policy Framework or Sender ID to check incoming emails,*
- *use of "hard fail" SPF TXT methods, DKIM and DMARC DNS records to block e-mails impersonating your organization,*
- *blocking untrusted/unapproved cloud computing services,*
- *logging recipients, size, number and frequency of e-mails sent,*
- *blocking and logging emails with sensitive phrases and data patterns,*
- *blocking messages containing attachments in the form of executable files;*

3 *Direct connections to the Internet from the institution devices should be prevented. Use a gateway firewall to enforce a separate DNS server, e-mail server, and Internet proxy server for outgoing network connections;*

4 *Use strong encryption mechanisms between e-mail servers or secure the e-mail itself (e.g., by encrypting it);*

5 *Use strong encryption mechanisms to protect sensitive data stored in systems and mobile devices;*

6 Use strong encryption mechanisms to protect sensitive data sent in ICT networks;

7 Protecting information on transactions made as part of the services provided by applications to prevent errors in transmission, routing, unauthorized changes to messages, unauthorized disclosures or reproduction, e.g., transaction details information should not be available from public networks.

PRACTICES

1. The institution should create a DMZ (demilitarized zone) as a perimeter network that protects and adds an extra layer of security to an organization's internal local-area network from untrusted traffic.

2. A demilitarized zone network is to allow an organization to access untrusted networks, such as the Internet, while ensuring its private network or LAN remains secure.

3. The institution should store in DMZ:

a) external-facing services and resources,

b) servers for the Domain Name System (DNS),

c) File Transfer Protocol (FTP),

d) e-mail,

e) proxy,

f) and web servers.

These servers and resources should be isolated and given limited access to the LAN to ensure they can be accessed via the internet, but the internal LAN cannot.

17.2 Enhanced Security Requirements

17-3. The institution separates user functionality from system management functionality.

17-4. The institution prevents unauthorized and unintended information transfer via shared system resources.

17-5. The institution implements subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

17-6. The institution denies traffic by default and allows traffic by exception (i.e., deny all, permit by exception).

17-7. The institution prevents remote devices from simultaneously establishing non-remote connections with organizational systems and communicating via some other connection to resources in external networks (i.e., split tunnelling).

17-8. The institution implements cryptographic mechanisms to prevent unauthorized disclosure of NPI during transmission unless otherwise protected by alternative physical safeguards.

17-9. The institution terminates network connections associated with communications sessions at the end of the sessions or after a defined period of inactivity.

17-10. The institution establishes and manages cryptographic keys for cryptography used in organizational ICT systems.

17-11. The institution uses strong cryptography when used to protect the confidentiality of NPI.

PRACTICE

Recommendation for strong cryptography mechanisms - See Appendix 1

17-12. The institution prohibits remote activation of collaborative computing devices (networked whiteboards, cameras, and microphones) and provides the information to the users when the device is enabled.

17-13. The institution controls and monitors the use of mobile code.

PRACTICE

Mobile code technologies include Java, JavaScript, ActiveX, Postscript, PDF, Flash animations, and VBScript. Decisions regarding the use of mobile code in organizational systems should base on the potential for the code to cause damage to the systems if used maliciously. Mobile code policy and procedures address controlling or preventing the development, acquisition, or introduction of unacceptable mobile code in systems, including requiring mobile code to be digitally signed by a trusted source should be developed.

17-14. The institution controls and monitors Voice over Internet Protocol (VoIP) technologies.

17-15. The institution protects the authenticity of communications sessions.

17-16. The institution protects the confidentiality of NPI at rest.

17-17. The institution protects its web application against cyber threats inherent in web technologies.

PRACTICE 1

Proper design and implementation of web applications, along with their deployment on secure execution platforms (e.g., PHP, Java, etc.) and application servers (such as Apache, Glassfish, WebSphere, WebLogic, etc.), contribute to their resilience against cyberattacks, including those listed in OWASP Top 10. However, given the possibility of new vulnerabilities being discovered in these platforms, servers, or even within the applications themselves (as revealed during penetration testing), organizations are encouraged to consider the deployment of Web Application Firewall (WAF) solutions to provide an additional layer of protection for their web applications.

PRACTICE 2

Similar to secure connections to Websites, an institution should ensure secure communication with API interfaces. To implement it, the following steps should be considered but not limited to:

1. *Use HTTPS protocol instead of HTTP for secure communication. HTTPS encrypts the data in transit between the client and server, preventing eavesdropping and tampering with the data.*
2. *Implement a secure authentication and authorization mechanism to ensure only authorised users can access the API. Consider using tokens, OAuth2 protocol, or API keys.*
3. *Validate all user input to prevent any malicious activity via API access.*
4. *Validate all input data to prevent injection attacks such as SQL injection or Cross-Site Scripting (XSS) attacks.*

5. *Implement rate-limiting to prevent DoS attacks by limiting the number of requests a user can make in a given time period. This might be done by configuring the network devices.*
6. *Keep logs of all requests and responses to the API, and monitor them for any suspicious activity.*
7. *Use the latest security standards: Ensure that the API is using the latest security standards and protocols, such as TLS 1.2 or higher, and avoid using deprecated or weak cryptographic algorithms.*
8. *Conduct regular security tests and audits to identify any vulnerabilities or weaknesses in the API and promptly address them.*

18 System and Information Integrity

18.1 Basic Security Requirements

18-1. The institution identifies, reports, and corrects system security flaws on time.

18-2. The institution protects malicious code (malware) within organizational ICT systems and updates malicious code protection mechanisms when new releases are available. Detected malicious software is addressed.

PRACTICES

Protection against malware should rely on the use of a number of the following technical and organizational measures:

1 In order to identify malware, it is necessary to update the antivirus software in use;

2 Before running a file, its prevalence and digital signature should be checked, e.g., using anti-virus software based on heuristics and reputation assessment;

3 Trusted software that prevents the execution of malicious code by blocking .exe files, DLL files, scripts (e.g., Windows Script Host, PowerShell and HTA) and installers should be used. White lists of allowed applications can be used for this purpose;

4 In the case of systems for which it is not possible to implement the recommended security patches, other security measures should be planned and implemented to ensure an appropriate level of security;

5 Configure macro support in Microsoft Office software to block macros in documents downloaded from the Internet and allow only tested and approved macros, or allow macros to run in a "secure environment" with limited write rights or digitally keyed macros from a trusted source;

6 Applications that require Java should be run after adding them to the list of safe applications or using certificates.

18-3. The institution monitors system security alerts and advisories and takes action as soon as they are published.

18.2 Enhanced Security Requirements

18-4. The institution performs periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

18-5. The institution monitors organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

19 PII Processing and Transparency

19.1 Basic Security Requirements

19-1. The institution identifies and meets the requirements for preserving privacy and protecting PII according to applicable laws and regulations and contractual requirements.

19-2. The institution complies with the current law relating to the protection of personal data and privacy in Rwanda.

20 Contingency Planning

20.1 Basic Security Requirements

20-1. The institution ensures that backup copies of data, software and system images are regularly made and tested.

PRACTICES

Backup copies of data, software and system images should be regularly made and tested as follows:

1 Procedures must be developed for backing up and testing data (any relevant, new and changed data), software and systems (including device configurations);

2 The occurrence of execution, storage time, type of backup (incremental, complete), and mode of backup (online, offline, offsite) should depend on the nature of the system, the amount and significance of the processed information and/or the number of irreversible changes;

a) Offline backup is a method of backing up your data to a local device, such as an external hard drive, USB flash drive, or optical disc. Offline backup is fast and secure, but it may require manual intervention and may be susceptible to physical damage, theft, or loss.

b) Offsite backup is a method of backing up your data to a different physical location than your primary data source, such as another office or a data center or another designated institution's premises. Offsite backup is useful for protecting your data from disasters, such as fire, flood, or theft, but it may be costly and time-consuming to transport and store your data.

c) Online backup is a method of backing up your data to a remote server. Online backup is convenient and accessible, but it may require a fast and reliable internet connection and may be vulnerable to hacking or data breaches.

3. There are following types of backups in terms of the process of copying the data. It should be noted that each institution should make a decision on what type of backup should be used based on the risk analysis:

a) Full Backup: This is the simplest backup form that copies all system data. It provides the highest level of protection but also requires the most storage space and backup time.
b) Incremental Backup: This type of backup only copies the data that has changed since the last backup. It is more efficient regarding storage space and backup time than a full backup, but restoring data from incremental backups can be more time-consuming.
c) Differential Backup: This type of backup copies all data that has changed since the last full backup. This means it stores more data than an incremental backup but less than a full backup. The restoration process is usually faster than with incremental backups.
d) Mirror Backup: This is a real-time backup that instantly copies any changes made to the data. It's similar to a full backup but doesn't store old versions of files.
e) Snapshot Backup: This type of backup creates a snapshot or a point-in-time copy of the system data. It's useful for backing up databases or systems that are constantly changing.

f) Continuous Data Protection (CDP): This type of backup continuously captures changes to the data, allowing for more granular recovery point objectives (RPO).

g) Synthetic Full Backup: This is a process in which a full backup is synthesized by taking an initial full backup and combining it with subsequent incremental backups.

4 Copies should be encrypted and stored in a dedicated space with limited access to the organization's network and no Internet access. Copies should cover at least the period before and after each configuration change, patch upload, etc.;

5 The correctness of backup and recovery should be tested at regular intervals and in the event of major changes to the ICT architecture;

6 Procedures should be developed for making and storing data backups in a different location (outside the facilities belonging to the institution), the loss of which may disrupt or prevent the functioning of the institution's ICT infrastructure.

20.2 Enhanced Security Requirements

20-2. The institution establishes, maintains, and effectively implements plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

PRACTICES

An institution's readiness for business continuity should include:

1 Implementation of information processing facilities (network devices, servers, other critical devices) with redundancy sufficient to meet availability requirements;

2 Performing Business Impact Analysis and risk assessment to identify critical processes and resources (data, ICT systems, facilities, devices, employees, third party suppliers/services, etc.);

3 Developing a business continuity strategy that involves using own or an external Disaster Recovery Center (e.g., public cloud);

4 Organizing a response structure;

5 Preparing warning and communication plan/procedures;

6 Creating business continuity plans and procedures;

7 Testing business continuity plans and procedures;

8 Continuous improvement.

21 Supply Chain Risk Management

21.1 Basic Security Requirements

21-1. In collaboration with a competent authority where applicable, the institution establishes and agrees on information security requirements with each supplier based on the type of supplier relationship.

PRACTICE

In addition to the requirements regarding ICT security, legal requirements, e.g., regarding the protection of personal data, should also be taken into account.

21-2. In collaboration with a competent authority where applicable, the institution defines and implements processes and procedures to manage the information security risks associated with the use of supplier's products or services.

21.2 Enhanced Security Requirements

21-3. In collaboration with the competent authority where applicable, the institution defines and implements processes and procedures to manage the information security risks associated with the ICT products and services supply chain.

21-4. The institution, in collaboration with the competent authority where applicable, regularly monitors, reviews and audits the provided external services.

PRACTICES

The institution should consider the following risk factors during the preparation of contracts with providers of ICT services and products:

1 When selecting a service provider, its current financial and economic situation should be taken into account, and the ownership structure should be examined, if possible, including the identification of real beneficiaries;

2 Every relationship with a new partner should start with a confidentiality agreement. Such an agreement should provide for real sanctions in the event of its violation. Particular attention should be paid to relations with suppliers of ICT solutions or products containing computer software that may affect the operational capacity of the institution's IT infrastructure;

3 Each concluded contract should be subject to risk analysis regarding the so-called vendor lock (VL), i.e., dependence on one supplier. VL is usually associated with unfavourable intellectual property provisions regarding the possibility of developing or using products (usually software) in the event of the supplier's bankruptcy or termination of cooperation by the supplier. The solution recommended for key ("tailor-made") ICT systems is the transfer of proprietary copyrights to the extent that allows modification of the software or the provision of a long-term license enabling independent development of the software, including the possibility of entrusting it to

third parties. At least, the use of escrow[6] mechanisms for the source codes and development environment of a given application should be considered;

4 *The contract should contain a description of the expected scope of cooperation of the service provider, including third parties acting on its behalf, and co-participating in the provision of the service with the institution in the event of fixing failures. This scope should include, but is not limited to the provision of specific infrastructure, personnel and availability of such personnel;*

5 *Definitions of failures or errors used in contracts should take into account phenomena resulting from the detection of new software vulnerabilities;*

6 *The contract should contain rules for removing reported errors, in the form of the so-called Service Level Agreement (SLA), containing indicators regarding cooperation procedures, timeliness of removing reported errors as well as sanctions for delays in removing errors and their failure to remove them;*

7 *Service contracts with software developers/producers should include additional SLAs regarding the removal of detected vulnerabilities, the use of which may cause the risk of disrupting the functioning of the institution's ICT infrastructure;*

8 *Depending on the identified significance of the impact of the software on the functioning of the institution's ICT infrastructure, it is advisable to regulate access to the source code of the institution by authorized personnel or an auditor selected by the parties, both during the term of the contract and after its completion;*

9 *The contract for the supply or maintenance of software should contain provisions regarding the procedure for managing changes in this software and the method of determining the service provider's remuneration for this;*

10 *The contract should contain sanction mechanisms, giving the institution financial (e.g., deductions, contractual penalties) or organizational (e.g., termination of the contract) rights in the event of a breach of obligations by the supplier;*

11 *The contract should not contain provisions completely excluding the supplier's liability or limiting its liability to amounts that do not correspond to the risk associated with the delivery of a product or service that does not meet the contract conditions;*

12 *The contract should include (in the case of ICT systems supporting critical processes) the requirement for the supplier to have an insurance policy against losses caused by improper performance of the contract;*

13 *The agreement should have a formalized escalation path in solving problems arising from the implementation of the agreement, including a procedure enabling immediate action in the event of threats to the institution resulting from attacks on ICT infrastructure;*

14 *The contract for the supply of software and hardware should contain provisions increasing security against ICT threats, i.e.:*

- *obliging the supplier to check whether the delivered software and hardware do not have known security gaps and to inform the ordering party about any existing gaps,*

[6] Access to codes via escrow - securing the company's interests by entrusting a third party with the source codes of a given IT solution. In the event of bankruptcy of the software supplier, the third party transfers the source code to the service recipient/ordering party

- *declaration that the architecture of the delivered software makes it possible to remove any security gaps that will be discovered during the software life cycle,*
- *the attached list of all components of the delivered software,*
- *additionally, it is recommended that the agreement be accompanied by declarations of software developers or hardware manufacturers regarding the rules they use to remove detected security gaps, the rules for informing users about detected security gaps and the rules for distributing patches.*

21-5. In collaboration with the competent authority where applicable, the institution regularly monitors, reviews, evaluates and manages changes in a supplier's information security practices and service delivery.

PRACTICE

In collaboration with the competent authority where applicable, an institution should specify security mechanisms, service levels and management requirements in all its network service contracts. If outsourcing services are used, the service provider should be obliged to implement an event logging system in networks and ICT systems and develop procedures for archiving the collected logs (at least for a period of 12 months).

22 References

[LAW 058/2021] Law Nº 058/2021 of 13/10/2021 relating to the protection of personal data and privacy in Rwanda.

[LAW 26/2017] Law No 26/2017 of 31/05/2017 establishing the National Cyber Security Authority and determining its mission, organisation and functioning.

[LAW 017/2020] Law No 017/2020 of 07/10/2020 establishing the general statutes governing public servants

[GOV] ICT Implementation Guidelines for GoR. Rwanda Information Society Authority, 2019

[NIST800-171] NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, February 2020

[NIST800-53] NIST Special Publication 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations

[ISO27000] ISO/IEC 27000:2009 Information technology — Security techniques — Information security management systems — Overview and vocabulary

[ISO27002] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection – Information security controls

[ISO27001] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

[ISO27005] ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks

[ISO19011] ISO 19011:2018 Guidelines for auditing management systems

[ISO17021] ISO/IEC 17021-1:2015 Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements

[ISO31000] [31000] ISO 31000:2018 Risk management – Principles and guidelines

[ISO22301] ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements

[ENISA-1] ENISA Technical guidelines for implementation of minimum security measures for Digital Service Providers, December 2016

[ENISA-2] ENISA Technical Guideline on Security Measures - Technical guidance on the security measures in Article 13a, Version 2.0, October 2014

[ISO27110] ISO/IEC TC 27110:2021 Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines

[FICIC] Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, NIST, April 16, 2018

[TR-02102-1] Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 1 – Cryptographic Mechanisms: Recommendations and Key Lengths, Version 2023-01

[TR-02102-2] Technical Guideline TR-02102-2 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 2 – Use of Transport Layer Security (TLS), Version 2023-01

[TR-02102-3] Technical Guideline TR-02102-3 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 3 – Use of Internet Protocol Security (IPsec) and Internet Key Exchange (IKEv2)

[TR-02102-4] Technical Guideline TR-02102-4 Cryptographic Mechanisms: Recommendations and Key Lengths, Part 4 – Use of Secure Shell (SSH)

23 Appendix 1 - Cryptographic controls

23-1. Organization provides transmission confidentiality and integrity. System and network administrators are responsible for appropriate configuration of cryptographic mechanisms on servers and network devices according to the requirements presented in Table 4.

Area	Protocols and algorithms
Recommended Cryptographic Mechanisms & Key Lengths	See Technical Guideline TR-02102-1 [TR-02102-1]
Network connection via public network using TLS protocol	TLS 1.2, TLS 1.3[7] or HTTPS based on them with: ⇨ cipher suites, ⇨ Diffie-Hellman groups, ⇨ signature algorithms, ⇨ Hash functions, ⇨ Other restrictions, required in Technical Guideline TR-02102-2 [TR-02102-2]. Authentication of the communication partners should base on X.509 certificates and depends on the application: a) When using TLS on the web, at least an authentication of the server is generally necessary, but server certificate must be issued by Trusted Certification Authority (TCA); b) When using TLS in closed systems (VPN or the like), authentication on both sides is usually required and certificate issuer can be TCA or internal if both sides agreed.
Network connection via public network using IPSEC protocol	IPSEC with IKEv2 with Perfect Forward Secrecy and: ⇨ Encryption algorithms, ⇨ pseudo random functions for key generation ⇨ functions for the protection of the integrity of IKE messages ⇨ groups for the Diffie-Hellman key exchange ⇨ authentication methods, required in Technical Guideline TR-02102-2 [TR-02102-2]. Authentication of the communication partners should base on X.509 certificates. When using TLS in closed systems (VPN or the like), authentication on both sides is usually required and certificate issuer can be TCA or internal if both sides agreed.

[7] TLS 1.0, 1.1 and SSL are not recommended since these protocols contains cryptographic vulnerabilities

	IPSEC protocol with: ⇨ ESP packets encryption methods, ⇨ ESP packets integrity methods, ⇨ AH packets integrity methods, ⇨ SA lifetime and rekeying. required in Technical Guideline TR-02102-3 [TR-02102-3].
Connection to system and devices using ssh protocol	SSH version 2.0[8] with: ⇨ Key agreement, ⇨ Key re-exchange, ⇨ Encryption algorithms, ⇨ MAC protection, ⇨ Server authentication, ⇨ Client authentication, ⇨ Other restrictions, required in Technical Guideline TR-02102-4 [TR-02102-4].
Hard disk encryption in mobile computers	BitLocker for Windows or file encryption on Linux with minimum AES 256 bit.
Media encryption in case of their transportation	File encryption using a tool (e.g., 7-zip) with minimum AES 256 bit.

Table 4 – Cryptographic requirements

23-2. Alternative to hard disk encryption in mobile computers or media encryption, the institution may prohibit carrying them out in case of their transportation or require strict and continuous physical control outside the institution's controlled facility.

[8] SSH-1 is not recommended since this protocol version contains cryptographic vulnerabilities.

24 Appendix 2 - Secure application coding principles[9]

The institution should establish processes to provide good governance for secure coding. A minimum secure baseline should be established and applied. Additionally, such processes and governance should be extended to cover software components from third parties and open-source software.

The institution should monitor real world threats and up-to-date advice and information on software vulnerabilities to guide the institution's secure coding principles through continual improvement and learning. This can help with ensuring effective secure coding practices are implemented to combat the fast-changing threat landscape.

1. Planning and before coding

Secure coding principles should be used for new developments and in reuse scenarios. These principles should be applied to development activities, both within the institution and for products and services supplied by the institution to others. Planning and prerequisites before coding should include:

a) establishing and communicating clear secure coding expectations, encompassing approved principles and guidelines aligned with industry best practices, for both in-house and outsourced code development;

b) analyzing and documenting common and historical coding practices and defects, such as insecure authentication and session management, improper error handling, security misconfiguration, weak cryptographic practices among others, which have led to security vulnerabilities;

c) ensuring proper configuration of development tools, including integrated development environments (IDEs), to enforce secure coding practices;

d) following guidance issued by the providers of development tools and execution environments as applicable;

e) regularly updating and maintaining the development tools, compilers, libraries, and frameworks used in the development process;

f) ensuring the qualification of developers in writing secure code;

g) integrating security considerations into the design and architecture of the application or software, and conduct threat modeling to identify potential threats and vulnerabilities, and plan for mitigation measures;

h) enforcing secure coding standards, and mandating their relevant use;

i) use of controlled environments for development such as sandbox or isolated environments, to mitigate the risks associated with developing and testing potentially vulnerable code.

2. During coding

[9] This appendix bases on [ISO27002, clause 8.28]

Considerations during coding should include:

a) secure coding practices specific to the programming languages and techniques being used;

b) using secure programming techniques, such as pair programming, refactoring, peer review, security iterations, and test-driven development;

c) using structured programming techniques by adhering to the principles that improve code clarity, maintainability, and security;

d) documenting code and removing programming defects, which can allow information security vulnerabilities to be exploited;

e) prohibiting the use of insecure design techniques (e.g., the use of hard-coded passwords, unapproved code samples, and unauthenticated web services).

Testing should be conducted during and after development. Static application security testing (SAST) processes can identify security vulnerabilities in software.

Before software is made operational, the following should be evaluated:

a) the attack surface of the software, identifying potential entry points and assessing the associated security risks, while adhering to the principle of least privilege;

b) conducting an analysis of the most common programming errors and documenting that these have been mitigated.

3. Review and maintenance

After the software has been made operational:

a) updates should be securely packaged and deployed;

b) reported information security vulnerabilities should be handled;

c) errors and suspected attacks should be logged and logs regularly reviewed to make adjustments to the code as necessary;

d) source code should be protected against unauthorized access and tampering (e.g., by using configuration management tools, which typically provide features such as access control and version control).

If using external tools and libraries, the public institution should consider:

a) ensuring that external libraries are managed (e.g., by maintaining an inventory of libraries used and their versions) and regularly updated with release cycles;

b) selection, authorization and reuse of well-vetted components, particularly authentication and cryptographic components;

c) examining the licenses, security, and community support of external components;

d) ensuring that software is maintainable, tracked and originates from proven reputable sources;

e) the availability and continuity of development resources, including personnel, expertise, and artefacts, to ensure long-term support and maintenance of the software.

Where a software package needs to be modified, the following points should be considered:

a) the risk of built-in controls and integrity processes being compromised;

b) the need to obtain consent from the software vendor before modifying the software package and consider contractual or legal obligations;

c) the possibility of obtaining the required changes from the vendor as standard program updates;

d) the impact if the institution becomes responsible for the future maintenance of the software as a result of changes;

e) the compatibility with other software in use, ensuring that integration and interoperability are not compromised.