THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE - PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

Document Title

eGovernment Security Architecture – Standards & Technical Guidelines

Document Number

eGA/EXT/ISA/001

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Jabiri Bakari	CEO – eGA		

Version: 1.0 – February 2016

Table of Contents

1. OVERVIEW 2
1.1 Introduction 2
1.2 Rationale 2
1.3 Purpose 3

2. EGOVERNMENT ICT SECURITY ARCHITECTURE 3
2.1 Technical Reference Model 3
2.2 eGovernment Security Architecture Standards 10
2.3 eGovernment Security Architecture Technical Guidelines 17

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT 43

4. GLOSSARY AND ACRONYMS 43
4.1 Glossary 43
4.2 Acronyms 43

5. RELATED DOCUMENTS 44

6. DOCUMENT CONTROL 45

APPENDIX 46

1. OVERVIEW

1.1 Introduction

Modern functioning of the Government is greatly contributed by ICT. Today, most of Public Institutions business operations rely on ICT much more than in the past. As Public Institutions deploy ICT systems, it becomes important to share information and make the systems interoperable, making reliability of business operations to ICT unavoidable. The security of ICT, is therefore of outmost importance and if not properly addressed, the business operations are put at risks of unavailability, and become unreliable. It is imperative to efficiently and effectively address ICT security issues and eGovernment Security Architecture is one of the methods to do that.

This document is provides eGovernment Security Architecture, Standards and Technical Guidelines. It provides low levels of eGovernment Security Architecture (Technical levels) and it is based e-Government Enterprise Architecture. It is a key tool for improving information security planning, implementation and operations on integrated information systems environment. It improves the ability to make security design decisions that are aligned with business requirements. The ICT Security architecture is a continuous process, rather than a one-off activity. The focus is on developing and maintaining a set of evolving requirements, models, templates and principles, rather than delivering a set of static artefacts.

The Security Architecture Standards is a part of Technical Reference Model as derived from the e-Government Enterprise Architecture referred in *e-Government Architecture Vision - Standards and Guidelines*.

1.2 Rationale

The Security Architecture enable the Government to provide a framework that will provide guide in selecting, implementing, and managing Information Security Services by guiding Public Institutions on how to manage ICT assets and to secure business functions including public access to appropriate information and resource. All together protect both the flow of data and processes with stakeholders for the

purpose of protecting information confidentiality, integrity and availability of data throughout the ICT lifecycle.

1.3 Purpose

In line with the above rationale, the Security Architecture Framework aims to protect physical and electronic assets, resources, and data/information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

i. Integrity for guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity;
ii. Confidentiality for preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;
iii. Availability for ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, authorization and access control;
iv. Accountability , which includes requirements that actions of individuals or entities can be traced to the individual or entity, non-repudiation, and security review controls and procedures; and
v. Assurance, including security administration and adherence to security and infrastructure related standards.

2. eGOVERNMENT ICT SECURITY ARCHITECTURE

2.1 Technical Reference Model

eGovernment Security Architecture Standards forms part of the Technical Reference Model (TRM). TRM supports and enables the delivery of ICT Security Standards Domains and capabilities and provides a foundation to advance the re-use and standardization of technology and service components from a government-wide perspective. Aligning ICT capital investments to the TRM leverages a common, standardized vocabulary allowing cross departmental discovery, collaboration, and

interoperability. Public Institutions will benefit from economies of scale by identifying and re-using the best solutions and technologies to support their business functions, missions and target architecture. The TRM will continue to evolve with the emergence of new technologies and standards. The TRM has been structured hierarchically as:

i. Service Area – Each Service Area aggregates the standards and technologies into a lower-level functional area. Each Service Area consists of multiple Service Categories and Service Standards.

ii. Service Category – Each Service Category classifies lower levels of technologies and standards with respect to the business or technology function they serve. In turn each Service Category is comprised of one or more service standards.

iii. Service Standards – They define the standards and technologies that support a Service Category. To support Public Institutions mapping into the TRM, many of the Service Standardsprovide illustrative specifications or technologies as examples.

The following is the TRM for the Government.

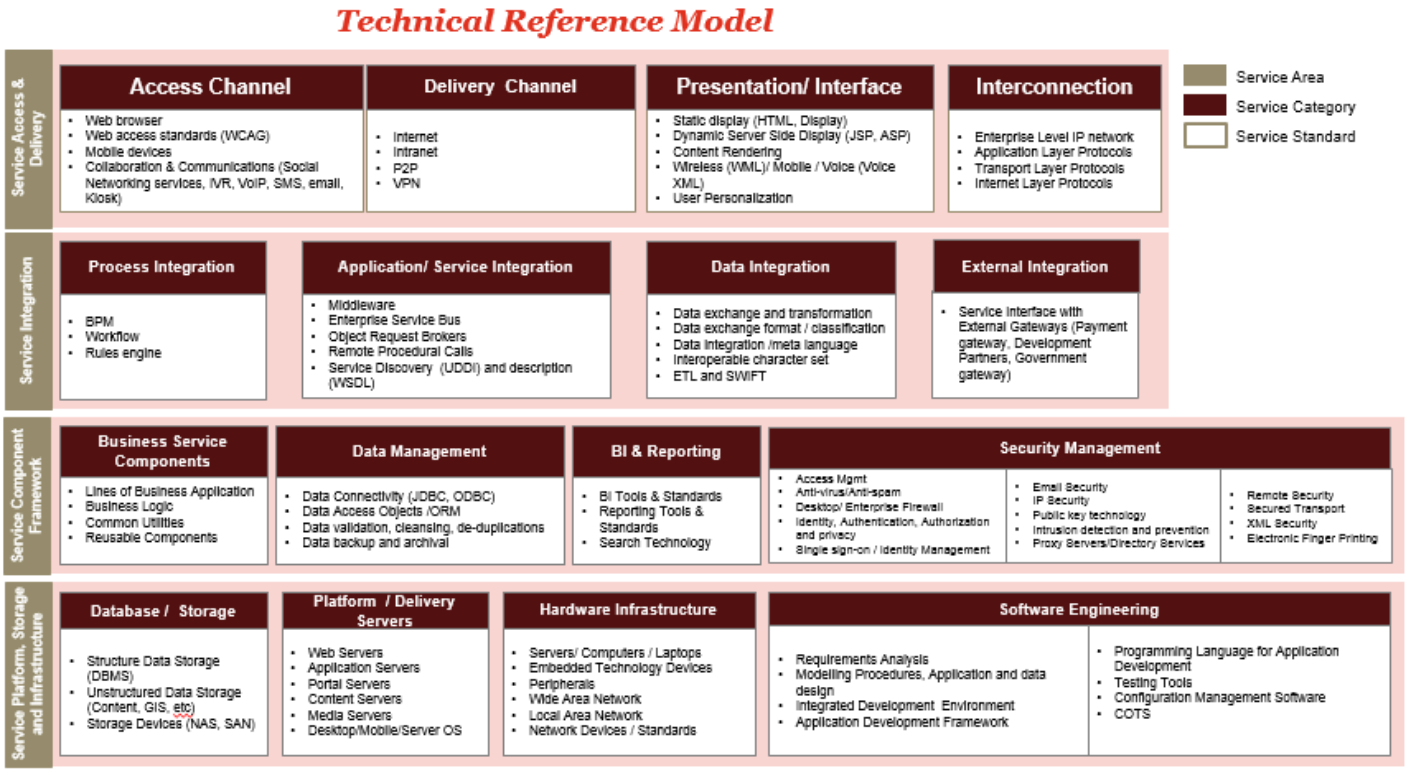

Figure I: Technical Reference Model

The TRM is standardised under 4 service areas:

i. Service Access and Delivery - This service area refers to the collection of standards and specifications to support external access, exchange and delivery of Service Components or capabilities.

ii. Service Interface and Integration - This service area refers to the collection of technologies, standards, and specifications that govern how Public Institutions shall interface both internally and externally with a service component. This area also defines the methods by which components shall interface and integrate with back-office/ legacy assets.

iii. Service Component Framework - This service area refers to the underlying foundation, technologies, standards, and specifications by which Service Components are built, exchanged, and deployed across Distributed or Service-Orientated Architectures.

iv. Service Platform, Storage and Infrastructure - This service area refers to the collection of delivery and support platforms, infrastructure capabilities and hardware requirements to support the construction, maintenance, and availability of a Service Component or capabilities.

Deriving from the TRM, the security measures to used across the above security layers are categorised and standardised across the entire Government in ten (10) Government ICT Security Domains (GISD).

i. ICT Security Governance and Management
ii. ICT Security Operations
iii. ICT Asset Management
iv. Identity and Access Management
v. ICT Security Incident Management
vi. Information Systems Continuity Management

vii. Security of Information Systems Acquisition, Development and Maintenance
viii. Human Resource Security
ix. Physical and Environment Security
x. Compliance and Audit

These domains are has been presented in the below;

Security Architecture Standards defines how the Public Institutions will securely and economically protect their business functions, including public access to appropriate information and resources, while maintaining compliance with the legal requirements established by existing statutes pertaining to integrity, confidentiality, accountability, availability, and assurance. From the information security domains, a security Reference Architecture Framework is derived. The Security Architecture Framework has been designed adhering to recommended overarching technology architecture principles (e.g. security, privacy and data protection) and Government ICT Security Domains (GISD).

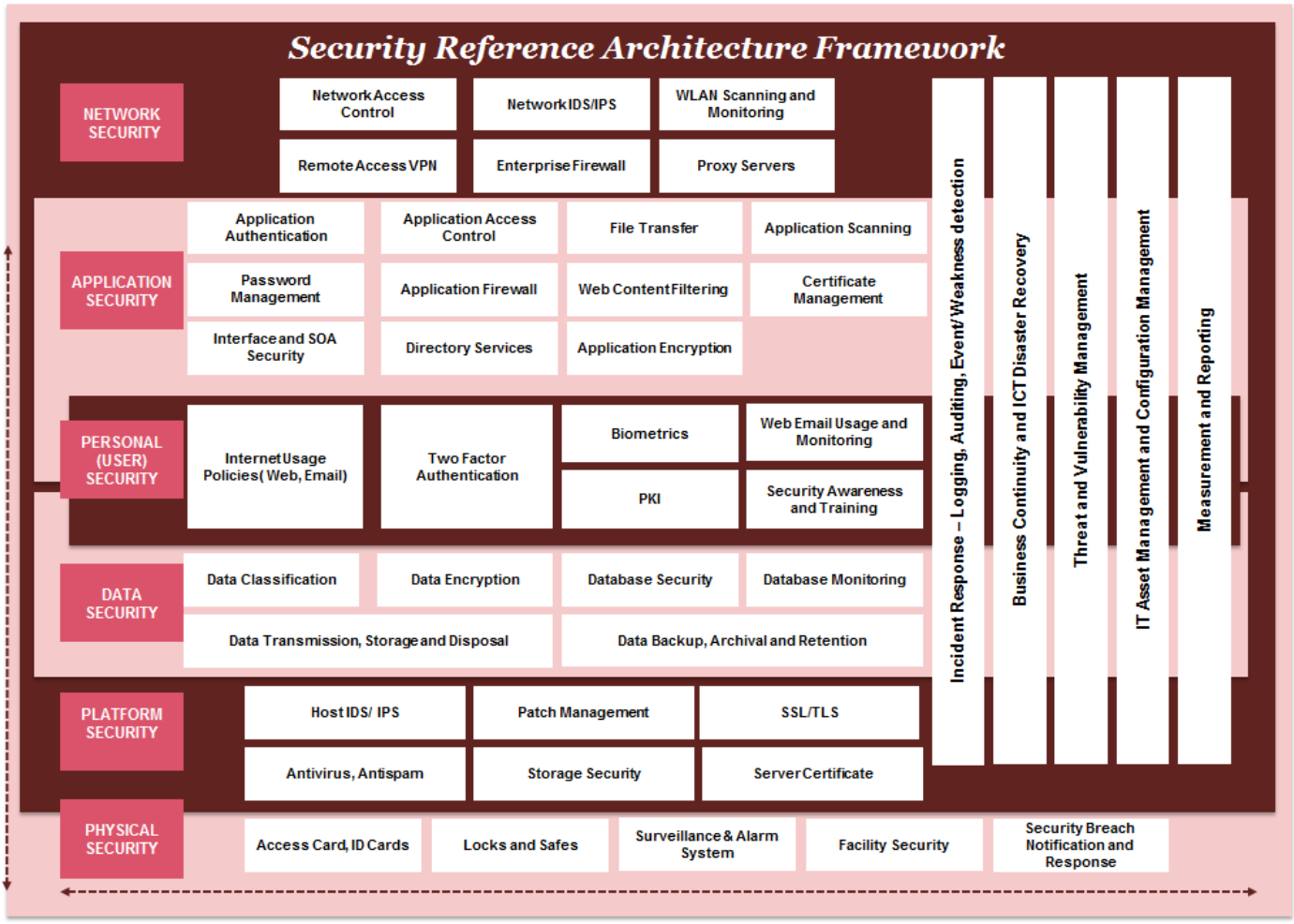

Figure II: Security Reference Architecture Framework

The following are details of the core layers described in the above diagram.

Table I: Details of the core layers described in Security Reference Architecture Framework

Security Layers	**Description**
Network Security	Network security deals with the security mechanisms adopted for the network considering network local/remote access control, authentication, firewall protection, network intrusion detections, and security

Security Layers	Description
	administration used by the Public Institution's ICT Operations and users
Application Security	Application security is the use of software, hardware, and procedural methods to protect applications from external threats. Security measures built into applications and a sound application security routine minimize the likelihood that hackers will be able to manipulate applications and access, steal, modify, or delete sensitive data.
Personnel/User Security	User security deals with the various aspects of security mechanism enforced at the end user level. It focuses on the user internet usage policies to be enforced and monitored, the various authentication mechanisms for verification of user identify such as two-factor authentication, biometrics based authentication, increase security awareness among users and employees and conduct security training.
Data Security	Data security deals with security mechanism adopted for keeping data protected from corruption and unauthorized access to ensure data privacy while maintaining data confidentiality. Data is considered a primary asset and as such shall be protected in a manner commensurate to its value. Security and privacy shall focus on controlling unauthorized access to data.
Platform /Host Security	Platform security deals with the security mechanisms adopted on servers, workstations and operating systems.

Security Layers	Description
	It covers server access control, host intrusion detections, use of server and desktop based anti-virus, anti-spyware, software patch management, storage security, IP security, communications endpoint security etc.
Physical Security	Physical security refers to the security characteristics concerned with restricting physical access by unauthorized personnel (potential intruders) to controlled facilities (buildings, computer rooms, data centres etc.) along with the access systems and types of access controls used in those same facilities or sites.
Cross Pillars: i. Incident Response ii. Business Continuity and ICT Disaster Recovery iii. Threat and Vulnerability Management iv. ICT Asset Management v. Measurement and Reporting	Incident Response aims to address and manage any security breach or attack. Business Continuity and ICT Disaster Recovery describes the process and procedures a Public Institution will put in place to ensure that essential business functions and ICT operations can continue during and after a disaster. Threat and vulnerability aims to identify risks and mitigation control in the ICT environment. ICT Asset management is a set of business practices to manage ICT assets throughout their lifecycle. Measurement and reporting provides information on the health check of the ICT appliances and systems.

The core layers described in the above diagram of the Security Architecture have been mapped against 10 defined ICT security domains (GISD) as follows:

Table II: 10 defined ICT security domains (GISD)

ICT Security Domain	Security Layers
1. ICT Security Governance and Management	Cross Pillars - Measurement and Reporting
2. ICT Security Operations	Network Security, Application Security, Data Security, Platform/Host Security.
3. ICT Asset Management	Cross Pillars - ICT Asset Management
4. Identity and Access Management	Network Security, Application Security, Physical Security.
5. ICT Security Incident Management	Cross Pillars – Incident Response
6. Information Systems Continuity Management	Cross Pillars - Business Continuity and ICT Disaster Recovery, Threat and Vulnerability Management
7. Security of Information Systems Acquisition, Development and Maintenance	Application Security
8. Human Resource Security	Personnel/User Security
9. Physical and Environment Security	Physical Security
10. Compliance and Audit	Cross Pillars - Measurement and Reporting

2.2 eGovernment Security Architecture Standards

2.2.1 Principles

The following are Security Architecture design principles to be adhered to:

Table III: Security Architecture design principles

Principle #1	***Security Control Compliance, Selection & Standardization***
Rationale	i. Achieving a standards-based environment will reduce operational costs, improve interoperability and improve supportability. ii. Ensures security solutions are fit-for-purpose. iii. Avoids breaches of confidentiality.
Implications	iv. Public Institutions will develop their respective Information Security Policies which includes data security, application security, amongst others. v. The security controls defined will be compliant with the pre-defined Government Policies. vi. The selection of security controls will be based on a risk analysis and risk management decision. The process for selecting new controls will consider both the degree of risk mitigation provided by the control and the total cost to acquire, implement and maintain the control. vii. Selection of controls will be driven by the ability of the control to be applied uniformly across the Public Institution and to minimize exceptions.

Principle #2	***Levels of Security***
Rationale	i. Security controls will be applied to reduce risk to an acceptable level.
Implications	i. Information systems (including applications, computing platforms, data and networks) will maintain a level of security that is commensurate with the risk and magnitude of the harm that could result from the loss, misuse, disclosure or modification of information.

	ii. Separate centralized teams will be formed for Application, data and ICT Security as identified in the Process and Governance Standards and Technical Guidelines.

Principle #3	***Security Measurement***
Rationale	i. Allows errors to be corrected and system misuse to be minimized.
Implications	ii. Security controls will be reviewed or audited through qualitative or quantitative means for traceability and to ensure that risk is being maintained at acceptable levels. iii. Public Institutions will be able to prepare a Security Dashboard which includes all relevant information security KPIs to be presented to management on a regular basis.

Principle #4	***Use of Common User Authentication***
Rationale	i. Allows easy access to authorized users. ii. This approach avoids duplication of effort and achieves economies of scale.
Implications	i. Centralized authentication mechanism will be developed by Public Institutions. ii. Existing application will be changed so that they can use the centralized model for user authentication. iii. Use of a common User Authentication framework will be supported. This includes reuse of the same authentication framework for national portal login and registering services on the ESB, for both consumers and businesses.

2.2.2 Information Security Governance and Management

2.2.2.1 To implement ICT Security Governance provisions that will provide direction and oversight to Institution's ICT Security Strategy, the strategy must be aligned to the requirement of this standard which include

i. Setting and reviewing measurable objectives for their ICT Security strategy and making sufficient budgetary provisions to achieve those objectives. Strategic objectives will have a primary focus upon addressing areas of most significant risk, achieving compliance obligations and address business needs in a secure manner.

ii. Ensuring suitable resourcing is provided for the Public Institution's ICT strategy to be transacted. Also, appointing an Officer responsible for ICT Security who will undertake day-to-day management of the ICT security strategy, supported as necessary by additional security-related roles.

iii. Constituting an ICT Security Governance Committee (ISGC) to provide executive-level oversight for the Institution's ICT Security Strategy.

2.2.2.2 ICT Security Risk Management process will be used in identifying, analysing, responding to and monitoring the most significant Information Security-related risks that the Institution faces. Apply appropriate responses to the most significant risks having a bearing upon their Information Security posture. The responses should be aligned to the Control Standards found within this document.

2.2.3 ICT Security Operations

2.2.3.1 For ICT security operations ensure that:

i. Information systems shall be monitored, against an agreed Information Security baseline, for performance and compliance with the Institutions' Information Security Policies.

ii. Key information relating to information system activities shall be logged for future use.

iii. Information systems will be subject to regular data back-up and media shall be handled securely.

2.2.4 ICT Asset Management

2.2.4.1 For ICT asset management ensure that:

i. Records are kept regarding the purpose, location, ownership and usage of those information assets.

ii. Information assets are classified in accordance with the Government Policies.

iii. Information assets (both physical and logical) should have appropriate labelling applied to clearly communicate their information classification.

2.2.5 Identity and Access Management

2.2.5.1 For access management ensure that:

i. Users of information systems and information processing facilities are appropriately authenticated, with access and privileges granted on the basis of a verified business need.

ii. Institutions are responsible for monitoring access for appropriate usage and revoking access when no longer required, or when deemed no longer appropriate.

iii. Users of information systems and information processing facilities shall be informed as to their obligations and responsibilities for ICT Security.

2.2.6 ICT Security Incident Management

2.2.6.1 For security incident management ensure that:

i. Potential incidents are anticipated and planning is undertaken to ensure an appropriate incident response can be mobilised when required.

ii. Significant incidents should be reported to eGA for appropriate support to be rendered to the Public and to facilitate cross-governmental information sharing.

2.2.7 Information Systems Continuity Management

2.2.7.1 For Information System Continuity ensure that:

i. Entities shall develop resource and test Disaster Recovery Plan.

ii. For each information system, a Recovery Point Objective (RPO) and Recovery Time Objective (RPO) shall be defined.

iii. Continuity planning shall seek to ensure that the agreed RPO and RTO targets can consistently be met, under a range of potential operational and exceptional circumstances.

iv. The Information System Continuity Management should be aligned with Business Continuity Management for the Institution, where the latter exists.

2.2.8 Information Systems Acquisition, Development and Maintenance

2.2.8.1 For Information Systems Acquisition, Development and Maintenance ensure that:

i. Business requirements of new systems or enhancements specify security control requirements;

ii. Systems and associated controls are designed, developed, implemented and tested against those requirements.

2.2.9 Human Resources Security

2.2.9.1 Institutions will implement work design and working practices that provide for personnel with secure access to government information assets and make provision for an appropriate segregation of duties, as determined by risk assessment.

2.2.10 Physical and Environmental Security

2.2.10.1 Physical security for server rooms, offices, and facilities have to be designed and applied.

2.2.10.2 Physical protection against natural disasters, malicious attack or accidents have to be designed and applied.

2.2.10.3 Access points such as reception areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

2.2.10.4 Power and telecommunications cabling carrying data or supporting information services will be protected from interception, interference or damage by appropriate access control methods.

2.2.10.5 When Supplier/Vendor environment is used, it will be assessed and/or audited for Public Institution's business security requirements compatibility.

2.2.11 Compliance and Audit

2.2.11.1 Ensure that independent ICT security reviews are regularly performed as party of internal operations and where necessary using external reviewers.

2.2.11.2 Ensure that ICT operations and management comply with legal, contractual and ICT security requirements.

2.2.11.3 Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislations, regulations, contractual and business requirements.

2.3 eGovernment Security Architecture Technical Guidelines

2.3.1 The following are Security Architecture Framework, Network Security Guidelines:

i. Network Access Control - Users will be provided with access to the network and network services that they have been specifically authorized to use by adopting appropriate network access control mechanisms.

ii. Remote Access (VPN) – Policies and supporting security measures shall be implemented to protect information access through remote connections.

iii. Network IPS/IDS – Protect network architecture through the use of IPS/IDS adhering to the following:

   a. IDS/IPS systems shall be in place at the Institutional network boundaries.

   b. Timely update of the IDS/IPS signatures and patterns will be performed to detect malicious activities based on signatures and patterns.

   c. Clear roles and responsibilities shall be assigned for various operational activities relating to the management of the IDS/IPS systems.

iv. Institutions will implement a firewall to segregate ICT assets that external services or internal users may access.

v. WLAN Scanning and monitoring –Utilize strong encryption and authentication controls on their wireless local area networks (WLANs) to prevent unauthorised access on the network.

2.3.2 Application authentication - Adhere to standards related to Identification, Authentication and Authorisation by:

i. Developing and maintaining a set of consistent policies and procedures covering the identification, authentication and authorization of system users.

ii. Maintaining that all system users are:
   a. Uniquely identifiable to ensure accountability
   b. Authenticated every time access is granted to a system
   c. Aware of the access control policies and procedures

iii. Public Institutions shall analyse different authentication mechanism and determine which is realistically possible to use in the delivery of e-Services. In e-Services authentication mechanism shall be used based on the criticality of the service. Before defining a specific authentication mechanism Public Institutions shall evaluate the type of authentication required for a specific service. Additionally, various authentication levels shall be defined based on the need.

   i. **Authentication Level 0** - At this level user authentication is not required. Here data is considered as public and usually these are informational material. Any user or entity can access this information. At this level there is no requirement to confirm the electronic identity of the user. However for tracking purposes, Public Institutions can log the IP address.

   ii. **Authentication Level 1** - At this level the authentication required is of moderate complexity. Electronic identity of the user should be established by Public Institutions so that services are accessed by authorized users or entities. The authentication mechanism proposed for this level is a one

factor authentication key in the form of a password. Strong password complexity Policies should be enforced to ensure confidentiality and integrity of the data.

iii. **Authentication Level 2** - The authentication mechanism at this level requires a high degree of certainty about the correctness of the electronic identity of an entity or user. It is extremely crucial for Public Institutions that only authorized persons have access to the offered service. This includes the online services that handle sensitive personal data or carry out financial transaction. The authentication mechanism proposed for this level is two factor authentications, that is, user specific password *(Refer to the technical guidelines for password management in this document)* and one time password for each session to avoid phishing, interception and other attacks.

2.3.3 Develop an enterprise authentication model that is suitable and secure. *Refer to Appendix – Illustration No.1 Identity Management Authorisation Model for more details*. Broadly, identity management authentication model shall be of three (3) types as required:

i. Silo Model - Under this model, the identity provider and the service provider are the same

ii. Centralised Model – Under this model, a separate application or system acts as an exclusive user credential provider for all service providers.

iii. Federated Model - A federated model provides a single logon service across multiple applications with a single identifier.

2.3.4 Interface and SOA security – Consider following security considerations while using web services. This includes:

i. SSL/TSL

ii. XML Data Security
iii. Security Assertion Mark-up Language
iv. SOAP Message Security

2.3.5 Application access control – Adhere to strict application access control policies which clearly define the following:

i. Access application system functions shall be restricted in accordance with the access control Policiess of the Public Institution
ii. Access to the application should be based on a need to know basis and formal access from the application owner.
iii. Restrictions to access shall be based on individual business application requirements
iv. The following shall be considered in order to support access restriction requirements:
    a. provide menus to control access to application system functions;
    b. control which data can be accessed by a particular user;
    c. control the access rights of users, e.g. read, write, delete and execute;
    d. control the access rights of other applications;
    e. limit the information contained in outputs;
    f. provide physical or logical access controls for the isolation of sensitive applications, application data, or systems.

2.3.6 Web application firewalls (WAFs) – Adhere to following standards when implementing web application firewalls:

i. Most WAFs have a set of pre-built Policies to ensure that devices are secured against the most commonly identified application security risks. Public Institutions shall configure these appliances in a

'learning mode' whereby the devices learn the application calls that are authorised during setup and testing phases.

ii. The WAF shall be configured to analyse inbound and outbound data and make a decision to block or permit specific elements.

2.3.7 File Transfer – Define formalised file transfer protocols taking into consideration:

i. To protect transferred information from interception, copying, modification, mis-routing and destruction.

ii. Encryption mechanism to protect the confidentiality, integrity and authenticity of information.

iii. Agreements shall address the secure transfer of business information between the Public Institution and external parties.

2.3.8 Web content filtering – Configure the firewall to ensure all inbound and outbound internet traffic is secured.

2.3.9 Encryption – Create a standardized procedure for encrypting information which include the following tasks

i. Analyse the risks of not using appropriately effective encryption and hashing schemes to protect information among different application.

ii. Define the minimum encryption and hashing key length/algorithm/function combination that should be used.

iii. Make reference to recommendations provided by the National Institute of Standards and Technology (NIST)

iv. Analyse the requirement of using digital certificate across different application.

v. Modify the applications to use the new encryption standards.

2.3.10 Application scanning - Use authorized automated tools for scanning and reporting. Ideally application scanning can be at code based level (static code analysis) and at end product level (Penetration testing) should be performed for all applications and services before and

after deploying on production environment. Scanning of web applications is essential and critical to detect possible security issues.

2.3.11 Internet usage Policies - Define an acceptable usage policies to help users in understanding what is considered acceptable and unacceptable in the use of the Public Institutions ICT resources. It shall set out the required behaviours and actions when using the Public Institution ICT equipment, Intellectual Property or software including incidental personal use of ICT systems, email addresses and the Internet (including social networking) *Refer to ICT Acceptable Use Template Ref No: eGA/EXT/TEM/011*.

2.3.12 Biometrics - Make use of biometric mechanisms in line with legal requirements pertaining the security around personal information.

2.3.13 Public Key Infrastructure - Leverage on the Government PKI infrastructure once fully operational.

2.3.14 Data classification - Define a data classification level as per regulatory requirements. Data shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.

2.3.15 Data backup and recovery – Ensure there is a Data Backup and Recovery procedures to ensure business continuity.

2.3.16 Data transmission, storage and disposal – Adhere to data handling policies based on their data classification level which take the following key factors into consideration:

i. Data Storage - All data "at rest" whether on a local workstation, on a server or archived in whatever form shall be physically encrypted.

ii. Data Collection and Transmission - All data transmissions shall be through encrypted channels.

iii. Data Disposal - Data shall be disposed of consistently with its classification and lifecycle and consistent with the Public Institutions policies and procedures. Access control mechanisms shall also be utilized to ensure that only authorized users can access data to which they have been granted explicit access rights during the disposal process.

2.3.17 Database security - Conduct a review of the key security controls implemented in the databases. The assessment shall include reviewing database server configuration parameters, operations and related procedures and shall cover the following areas:

i. Access controls and allocation of privileges
ii. Usage of privilege accounts
iii. Auditing, logging and monitoring
iv. DBMS configuration
v. OS access and user management
vi. Roles allocation
vii. Backup and recovery
viii. Password management
ix. Database Security patches management
x. Roles and Grant allocation
xi. User tracking method and implementation
xii. Username and password structure
xiii. Standards for views and roles

2.3.18 Antivirus, Anti-spam - Implement appropriate detection, prevention and recovery controls to protect against malware combined with appropriate user awareness.

2.3.19 Patch management - Define a patch management process which is repetitive and resource intensive; whose success is measured through compliance during audits and absence of unplanned downtime.

2.3.20 Access card, ID cards - Access to the Institutions' premises needs to be controlled through appropriate access control and authentication mechanisms. All members of staff need to be issued a staff identification card / access cards that shall be worn visibly at all times.

2.3.21 Locks and safes - All media containing confidential information need to be kept in safes where access is strictly controlled.

2.3.22 Surveillance & alarm system - The premises of the Institution need to be equipped with the appropriate surveillance alarm systems that are operational on a 24x7 basis.

2.3.23 Facility Security - Design and apply physical security for offices, rooms and facilities.

2.3.24 Security breach Notification and Response - Define process to ensure that all security breaches are detected on a timely basis and appropriate actions are taken accordingly.

2.3.25 Incident response – Adopt appropriate incident management Guidelines, policies and procedures in line to e-government standards and report any incidents to eGA.

2.3.26 Threat and vulnerability management – Perform regular threat and vulnerability assessment to discover and remedy security vulnerabilities on the ICT application and appliances to proactively prevent percolation of any threat vectors.

2.3.27 ICT asset and configuration management – Clearly identify all ICT assets and the purpose of same. This information shall be included in an asset register which is regularly updated. *Refer to ICT Service Management Template*

2.3.28 Measurement and reporting – Identify key security performance indicators that will be compiled and reported to the management team on a regular basis. The reporting structure should be clearly defined highlighting all roles and responsibilities.

2.3.29 Adhere to ICT Security, Standards and guidelines to develop institutional specific security programme and strategy which needs to be aligned to the security framework and industry standards such as ISO 27001 and ISO 27002, NIST 800 and ITIL. ICT Security should be incorporated across all stages of ICT project and portfolio management.

2.3.30 Perform an ICT risk assessment based on internal standards such as ISO 31000 which shall cover (but not limited to) security planning, security requirement definition, security evaluation criteria and continuous improvement and support. *Refer to Information Security Risk Assessment Template.*

2.3.31 Adopt enterprise licensing models for institutional application portfolio and leverage on government licensing agreements to reduce total cost of ownership. Preferably, suitably licensed software may be used in all Public Institutions.

2.3.32 Adhere to the Information Security Policies Template

2.3.33 All items of equipment being disposed of containing storage media should be verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use.

Leverage on digital signature to validate the authenticity and integrity of a message or digital document.

2.3.34 Consideration needs to be made in deploying data loss prevention mechanism to prevent unauthorized access and distribution of information.

2.3.35 Audit trails or audit logs need to be maintained by Institutions. Log information is critical in identifying and tracking threats and compromises to the environment. There are a number of devices and software that shall be logged which include hardware and software based firewalls, web servers, application servers, portal servers, authentication servers, central/domain controllers, database servers, mail servers, file servers, routers, DHCP servers etc.

2.3.36 Institutions will establish procedure for log management. While defining the procedure it is essential to decide what activities and events should be logged. The events which ideally should be captured include:

i. Create, read, update and delete of confidential records.
ii. User authentication and authorization activities e.g., user login and logout.
iii. Grant, modify or revoke user access rights including adding a new user or group, changing user privilege levels, changing file permissions, changing database object permissions, changing firewall policies, and user password etc.
iv. System, network or service configuration changes including installation of software patches and updates, or other installed software changes.
v. Application process start up, shutdown or restart, process abort, failure or abnormal terminations, failure of network services.
vi. Detection of suspicious activities such as from Intrusion Detection and Prevention system, anti-virus, anti-spyware systems etc.

2.3.37 Establish the standardized list of elements that should be captured as part of audit log information. The following elements are typically captured:

i. Type of action - examples include create, read, update, delete etc.
ii. Subsystem performing the action - examples includes process or transaction name, process or transaction identifier.
iii. Identifiers (as many as available) for the subject requesting the action - examples include user name, computer name, IP address and MAC address.
iv. Identifiers (as many as available) for the object the action was performed on - examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address.
v. Before and after values when action involves updating a data element, if feasible. Date and time the action was performed.
vi. Action status i.e. whether the action was allowed or denied by access-control mechanisms.
vii. Description and/or reason-codes of why the action was denied by the access-control mechanism, if applicable.

2.3.38 Considerations need to be made for establishing a plan to standardize the storage format of the logs captured so that it ensures the integrity of the log and support enterprise level analysis and reporting. Mechanisms known to support these goals include but are not limited to the following:

i. Event Logs collected by a centralized log management system; Logs in a well-documented format centralized log management system;
ii. Logs stored in an ANSI-character set database that itself generates audit logs in compliance with the requirements of this document.

2.3.39 Provide access to the network and network services only to users that they have been specifically authorized to use.

2.3.40 Have a formal authorisation process for the allocation and monitoring of privileged access rights.

2.3.41 Consideration need to be made for segregation of institutional network infrastructure into distinct segments Virtual Lan's (VLANS) based on the criticality of the systems. Communication between each network segment may be controlled by a firewall.

2.3.42 Conduct regular reviews to ensure compliance to the approved policies and regulatory and legal requirements (if any). Whenever possible, compliance checks should be conducted by independent reviewers.

2.3.43 Consideration need to be made for adapting a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.

2.3.44 Appoint external suppliers to conduct penetration tests on all internet facing applications.

2.3.45 Network Access controls

i. Identify networks and network services which are allowed to be accessed.
ii. Define authorisation procedures for determining who is allowed to access which networks and networked services.
iii. Identify management controls and procedures to protect access to network connections and network services which include:
   a) The means used to access networks and network services (e.g. use of virtual private network or wireless network);

b) User authentication requirements for accessing various network services;

c) Monitoring of the use of network services.

2.3.46 Remote Access (VPN)

i. Identify the communications security requirements, taking into account the need for remote access to the internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system.

ii. Provide a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the stakeholders are authorised to access.

2.3.47 Configuration of enterprise/institutional firewall need to be as follows:

i. Packet Filtering - A Packet Filtering Firewall examines each packet that passes through it up to the network layer. This means that the upper four layers (Application, Presentation, Session, and Transport) are allowed into an internal network. The Packet Filtering Firewall looks at each packet and determines what to do with it based on a policy base the Institution has defined.

ii. Application Gateway Proxy - Application Layer Gateway, or better known as Proxies, function on the application level. Proxies' firewalls face the challenge that outside networks are continually growing and introducing new protocols, services and applications all the time. As this happens, the Proxy has a difficult time handling these extreme communications on networks.

iii. Stateful Inspection - Stateful Inspection gathers, stores, and manipulates information pertaining to all communication layers and from other applications. This means that Stateful firewalls can tell what stage a TCP connection is in (open, open sent, synchronized, acknowledged or established) whether packets have fragmented etc.

2.3.48 WLAN Scanning and monitoring

i. Maintain the physical security of wireless access points to protect against theft or access to the data port. All access points shall be kept in a physically secure location accessible only by authorised personnel.
ii. Ensure that all management consoles are kept in a physically secure location.
iii. The Service Set Identifier (SSID) of each access point shall be changed from the default factory settings to an identifier that is difficult to guess and difficult to associate with the Institution.
iv. Configure the wireless infrastructure for strong authentication using an EAP (Extensible Authentication Protocol).

2.3.49 Authentication mechanism - Considerations need to be made on the use of the following authentication mechanisms:

i. Usage of at least two of the following factors of authentication is considered strong authentication such as a password, PIN etc.
ii. Usage of smart card, hardware security token, cell phone etc.
iii. Usage of fingerprint, a retinal scan, or other biometric methods.

2.3.50 Application authentication - Authentication systems adopted by Institutions can be classified as single, two or multidimensional, depending on the number of factors employed to ensure the desired level of certainty about the identity of an electronic entity.

i. Passwords - Passwords are the most widely accepted way of authentication where the user certifies the accuracy of identification using a secret known only to him. Typically, passwords shall be stored in an encrypted format in the user store.
ii. Disposable passwords - The distinctive single-use passwords are hardware devices that may be used to create passwords that will be used only once. The passwords shall be produced based on specific

ciphers. In this method, the reuse of code or password for future authentication of the user is not possible.

iii. Soft Tokens - These are secret keys which are stored electronically on media such as hard drives, CD, USB sticks etc. The keys are stored in an encrypted form and access to information is only possible with this key.

iv. Hardware Tokens - Hardware token is a physical device that a user has to use during authentication. The token acts like an electronic key to access information.

v. Biometric - Biometric refers to authentication techniques that rely on measurable physical characteristics that can be checked. Biometric authentication has been widely regarded as the most fool proof and hardest to forge or spoof. There are number of biometric methods such as fingerprint recognition, eye scan, signature dynamics, typing pattern, palm geometry, voice recognition, facial recognition etc.

2.3.51 Password management policies – Adopt strong password mechanisms which include:

i. Public Institutions shall enforce robust password complexity policies, account lockout, password expiry and reset features. End users should have the capability to reset their passwords.

ii. Public Institutions shall enforce a strong password policies with minimum password length of 8 characters consisting of lowercase characters, upper case characters, digits and special characters.

iii. Password shall be generated by the user except in the case of initial or reset password.

iv. Initial password shall be system generated using pseudo-random algorithm.

v. After authentication with the initial password user shall be forced to change his initial password.

vi. "Forgotten password services" capability shall be implemented to allow users to reset their password by answering knowledge based authentication questions.

vii. Password shall never be displayed on the screen.

viii. User shall be able to change the password at any time. While changing, the user shall enter the new password at least two times. If a user changes their password an email or notification should be sent to their registered email address or SMS that indicates a change has recently occurred on the user's profile.

ix. Ensure passwords are changed at most every 90 days and allow passwords to be reused within eight password changes.

x. Session timeout policies shall be enforced to automatically logout from the system after a definite period of inactivity. Users should be denied the ability to disable the timeout / system locking mechanism.

xi. Lock user account after five failed logon attempts and allow only system administrators to reset locked user accounts.

xii. User accounts shall be suspended at the earliest when the user no longer needs access to the system (either leaving the organization or due to change of role).

xiii. Sensitive authentication data shall be protected and stored in an encrypted form in the storage media.

2.3.52 For SOA Security adhere to the following guidelines:

i. Authentication - A user's identity is verified based on the credentials presented by that user, such as username/password, digital certificate, standard Security Assertion Mark-up Language (SAML) token, or Kerberos token. In the case of web services, credentials are presented by a client application on behalf of the end user.

ii. Integrity and non-repudiation

a) Address how message shall remain unaltered during transmission across all the various types of intermediary services.
b) Ensure an authority digitally sign that message; a digital signature also validates the sender and provides a time stamp ensuring that a transaction can't be later repudiated by either the sender or the receiver.
c) XML messages are signed using the XML Signature standard.

iii. Confidentiality - Address how data within a message can be protected so that it is not disclosed to unintended recipients while in transit. The message contents need to be encrypted independently from the transport as a part of the solution. This ensures that only intended recipients can access the protected data. A symmetric or asymmetric encryption and decryption algorithm specified in the XML encryption standard WS-Security should be enforced at the message level.

iv. Availability - Address how message should be promptly delivered to the intended recipient who ensures legitimate users receive the services they are entitled to.

2.3.53 Consideration need to be made for web service security design to cover the following core security aspects:

i. SSL/TSL - SSL/TLS is a cryptographic protocol that provides the security for communications over the network. SSL/TLS enables point-to-point secure sessions by providing server authentication to the client, optional client authentication to the server, data message authentication, data confidentiality, and data integrity.

ii. With respect to SSL, TLS incorporates an optional session caching scheme to reduce the number of connections that need to be established from scratch. Such optimization is intended to reduce the computational load introduced by encryption operations.

iii. In the case of web service a message transmitted by a client, such as browser or an application, might be routed and processed by a number of intermediary applications or services before reaching its final recipient. SSL/TLS protects the message contents only while they are being transmitted between pair wise endpoints. The message, once it is processed by SSL/TLS at a receiving end, is delivered decrypted to the application layer.

iv. XML Data Security - XML is the language to exchange data among Web services. Securing XML data by protecting their integrity and confidentiality as well as their authenticity, is a key requirement for web service security. Integrity and confidentiality can be achieved by using encryption mechanisms, while authenticity can be achieved by using digital signatures. XML encryption and XML Signature are the two ways to specify how to encrypt data and how to ensure the authenticity of the message using digital signature in a XML document.

v. XML Encryption - XML Encryption provides end-to-end security for applications that require secure exchange of structured data. It defines a standard model for following two areas:
   a. Encrypting part of the data being exchanged
   b. Secure sessions between more than two parties

vi. With XML encryption both secure and non-secure data can be exchanged in the same document. It can handle both XML and non XML data. While SSL/TLS provides confidentiality at the transport layer only, XML Encryption provides confidentiality at the application layer and thus assures end- to-end confidentiality of messages traversing multiple Web services.

vii. XML Encryption specification describes how to use XML to represent digitally encrypted Web resource (including XML data). The encryption information is stored separately from the encrypted data. Encryption information stores data about the encryption key and

encryption algorithm. XML Encryption can use PKI for encrypting data.

viii. XML Signature - XML Signature defines XML syntax for digital signatures. Like XML Encryption, it applies to both XML and non-XML data. The signed data items can be entire XML documents, XML elements, or files containing any type of digital data items. XML Signature allows one to sign multiple data with a single signature. XML signatures add authentication, data integrity, and support for non-repudiation to the data that they sign. XML-Signature allows different structures like enveloping signature, enveloped signature, and detached signature.

ix. Security Assertion Mark-up Language -Security Assertion Mark-up Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains. In SAML, security information is expressed as assertions about subjects, where a subject is an entity (either human or computer) that has an identity in some security domain. Assertions can convey information about the attributes of subjects, about authentications previously performed by subjects, and possibly about authorization decisions as to whether subjects are allowed to access certain resources.

x. SAML supports three kinds of assertions: attribute, authentication, and authorization decision assertions. A single SAML assertion might contain several assertion statements about authentication, authorization, and attributes. SAML can be used to make assertions about credentials.

xi. A service provider may need also to have detailed information about the type and strength of authentication used by an identity provider when it authenticated the user; to carry this information, SAML provides the authentication context, which is conveyed in (or referenced by) an assertion's authentication statement.

xii. SAML can support the following use cases.

a. Single sign-on (SSO) - Using SAML one can authenticate a user to an application who is already authenticated by another application. SAML carries the authentication information for the user from the first application to the second.

b. Authorization - Together with the authentication SAML can be used to decide the authorization for an entity. Like depending on the entity's role it can be decided whether a user can access a particular resource or not.

c. Securing SOAP messages - SAML assertions can be used within SOAP messages in order to carry security and identity information between entities in Web service transactions.

xiii. SOAP Message Security - SOAP is a protocol specification for exchanging structured information in the implementation of Web Services. Since a SOAP message can pass through multiple set of web service or application it can have security loopholes if proper measures are not taken. For example a message can be read by an attacker; a request can be tampered etc. Hence, there is the need to provide an end-to-end protection over multiple hops to assure SOAP message integrity and confidentiality, as well as to verify the requester's identity.

xiv. These goals can be achieved by using XML encryption and XML signatures.

xv. It is necessary to standardize the representation of the additional security information within SOAP messages themselves, so that the software component processing them, that is, the SOAP processor, can properly manage the security information.

xvi. Consider adhering to the following standards

a. WS-Security

b. WS-Security Conversions

c. WS-Reliability

2.3.54 Adhere to following Application firewall guidelines:

i. WAFs shall be considered in light of the application delivery, web services delivery and network security.

ii. WAF solutions may often be part of or provide a full suite of functionality to provide protection, and it is important for Public Institutions to assess their requirements and perform an appropriately detailed risk assessment when considering the appropriate WAF solution.

2.3.55 Security awareness and training - An information security awareness programme shall be established in line with the Public Institution's information security policies and relevant procedures, taking into consideration the Institution's information to be protected and the controls that have been implemented to protect the information.

i. The awareness programme shall include a number of awareness-raising activities such as campaigns (e.g. an "information security day") and issuing booklets or newsletters.

ii. Information security education and training shall take place periodically.

2.3.56 Data security classification - Adopt a data classification framework that:

i. Provides a standard data security classification process that will allow Institutions to evaluate their data assets and determine the appropriate level of security classification that shall be applied to these data assets thereby promoting interoperability. Consider leveraging the following approach:

   a. Identify information assets
   b. Identify the owner of the information asset
   c. Undertake impact assessment of information asset

d. Determine security classification scheme of the information assets
e. Apply security controls based on security classification
f. Document in security classified information register

ii. Provides a well-defined data classification schema that represents all of the types of data that exist or can exist in the environment. This includes:

a. Develop a simple set of criteria and a classification scheme for measuring information value.
b. When classifying information, each Information Owner should take into consideration the confidentiality, sensitivity, and privacy, legal, regulatory and access requirements of the information.
c. Develop a simple set of criteria and a classification scheme for measuring information value.
d. The business owners, in conjunction with the ICT Team, shall determine which data are critical to the operations of their department.

2.3.57 Adhere to the following Data classification levels guidelines in addition to existing regulatory requirements:

i. Top secret - This is the highest level of classification of data assets at the national level. Such information would cause 'exceptionally serious damage' to national security if made publicly available.
ii. Secret - Such information would cause 'serious damage' if made publicly available.
iii. Confidential - Such information would cause 'damage' if made publicly available.

iv. Restricted - Such information would cause 'undesirable effects' if made publicly available.

v. Unclassified - Information/documents which do not have any classification level listed could be place under 'Unclassified'. Such documents are publicly used and do not require any security controls to restrict access.

2.3.58 Adhere to following Antivirus, anti-spam guidelines:

i. Establish formal policies prohibiting the use of unauthorized software.

ii. Implement controls that prevent or detect the use of unauthorized software (e.g. application whitelisting).

iii. Implement controls that prevent or detect the use of known or suspected malicious websites (e.g. blacklisting).

iv. Establish a formal policies to protect against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken;

v. Reduce vulnerabilities that could be exploited by malware, e.g. through technical vulnerability management

vi. Conduct regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated;

vii. Installation and regular update of malware detection and repair software to scan computers and media as a precautionary control, or on a routine basis; the scan carried out should include:

a) Scan any files received over networks or via any form of storage medium, for malware before use.

b) Scan electronic mail attachments and downloads for malware before use; this scan should be carried out at different places,

e.g. at electronic mail servers, desk top computers and when entering the institution's network..

c) Scan web pages for malware.

2.3.59 Facility Security - The following guidelines should be considered to secure offices, rooms and facilities:

i. Key facilities should be cited to avoid access by the public.
ii. Where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building, identifying the presence of information processing activities.
iii. Facilities should be configured to prevent confidential information or activities from being visible and audible from the outside. Electromagnetic shielding should also be considered as appropriate
iv. Directories and internal telephone books identifying locations of confidential information processing facilities should not be readily accessible to anyone unauthorized.

2.3.60 Threat and vulnerability management – As part of the threat and vulnerability management, Institutions need to perform the following activities:

i. Identification of potential security threats and vulnerabilities within ICT environment and develop basic remediation process to actively monitor and manage perimeter security and critical internal systems.
ii. Deploy anti-virus software to all workstations and servers to reduce the likelihood of a security threats.
iii. Deploy perimeter and internal security appliances e.g., enterprise firewalls to reduce the likelihood of a security threats.
iv. Deploy web content filtering solutions to prevent threats from compromised websites to help identify and block potentially risky web pages.

v. To reduce vulnerability to phishing and other e-mail security spam, install enterprise-level e-mail anti security software that checks both incoming and outgoing messages to ensure that spam messages are not being transmitted if a system becomes compromised.

vi. To minimize the security risks due to use of removable media/ drives, apply simple preventative steps like disabling the "auto run" feature of the operating system on desktops/laptops and training users to scan removable media for viruses before opening the files.

vii. Periodic scanning of the network will identify system level vulnerabilities.

viii. Log information is critical to identifying and tracking threats and compromises to the environment. The granularity and level of logging shall be configured to meet security management's requirements. Establish processes for viewing logs and alerts.

ix. Deploy equipment to actively monitor and manage perimeter and internal information security. Establish security threat remediation and management processes to manage threat.

x. Deploy network Intrusion Detection System (IDS) on the perimeter and key points of the network and host IDS to critical systems.

xi. Deploy centralized process to correlate threat information from disparate sources.

2.3.61 Application scanning and testing – Adhere to following guidelines for application scanning and testing:

i. Define a risk rating matrix based on the Open Web Application Security Project (OWASP) to identify issues as most common and critical:

a. A1: Injection
b. A2: Cross-Site Scripting (XSS)
c. A3: Broken Authentication and Session Management
d. A4: Insecure Direct Object References

e. A5: Cross-Site Request Forgery (CSRF)
f. A6: Security Misconfigurations
g. A7: Insecure Cryptographic Storage
h. A8: Failure to Restrict URL Access
i. A9: Insufficient Transport Layer Protection
j. A10: Invalidated Redirects and Forwards

ii. Develop a plan for creating a centralized infrastructure to support application scanning. Application scanning is an iterative process, so it is important to capture metrics such as issues identified by application version and resolution at the application level as well as at the enterprise level.

iii. Create an authoritative source to inform developers on do's and don'ts and strengthen procedures in the Software Development Lifecycle (SDLC).

iv. Application Security Verification Standard - to adopt the application level security verification standards (ASVS) from The Open Web Application Security Project (OWASP). The primary aim of the OWASP Application Security Verification Standard (ASVS) is to provide a basis for testing application technical security controls, as well as any technical security controls in the environment, that are relied on to protect against vulnerabilities such as Cross-Site Scripting (XSS) and SQL injection. There are three main parts to OWASP ASVS. The requirements in ASVS define:

a. Levels of application-level security verification that increase in breadth and depth as one moves up the levels.
b. Verification requirements that prescribe a unique white-list approach for security controls.
c. Reporting requirements that ensure reports are sufficiently detailed to make verification repeatable, and to determine if verification was accurate and complete.

2.3.62 Development of Institutional **ICT Security Policy** should be as demonstrated in *"ICT Security Policy Template (eGA/EXT/TEM/002)"* also should be guided by the technical guidelines as described in "*Creation of ICT Security Policy – Technical Guide (eGA/EXT/ISA/003)"* .These are guidelines developed, for purpose of assisting the Head of ICT to develop the General ICT Security Policies of the Institution. The guide should be used to develop policies to suite Public Institution's need as directed by this.

2.3.63 A **Disaster Recovery Plan** with well-established Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of various business systems/applications and services needs to be developed as described in "*Disaster Recovery Plan – Technical Guide (eGA/EXT/ISA/002)"* document.

2.3.64 Further references (Templated and Technical Guides) related to e-Government Security Architecture will be developed from time to time.

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

3.1 This document takes effect once signed and approved in its first page.

3.2 This document is subject to review at least once every three years.

3.3 This Documents need to be complied with as directed in the most current version of "*Mwongozo wa Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya TEHAMA Serikalini".*

4. GLOSSARY AND ACRONYMS

4.1 Glossary

None

4.2 Acronyms

Abbreviation	Explanation
ASVS	Application Security Verification Standard

IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ITIL	Information Technology Infrastructure Library
MAC	Media Access Control
OWASP	Open Web Application Security Project
SAML	Security Assertion Mark-up Language
SDLC	Software Development Lifecycle
SOA	Service Oriented Architecture
SOAP	Simple Object Access Platform
SSL	Secure Socket Layer
TZ-CERT	Tanzania Computer Emergency Response Team
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
XML	Extensible Mark Up Language

5. RELATED DOCUMENTS

5.1. Mwongozo wa Matumizi Bora, Sahihi na Salama ya Vifaa na Mifumo ya TEHAMA Serikalini Toleo la 2

5.2. eGovernment Architecture Vision - Standards and Technical Guidelines *(eGA/EXT/AVS/001)*

5.3. eGovernment Interoperability Framework - Standards and Technical Guidelines *(eGA/EXT/GIF/001)*

5.4. eGovernment Business Architecture - Standards and Technical Guidelines *(eGA/EXT/BSA/001)*

5.5. eGovernment Application Architecture - Standards and Technical Guidelines *(eGA/EXT/APA/001)*

5.6. eGovernment Information Architecture - Standards and Technical Guidelines *(eGA/EXT/IFA/001)*

5.7. eGovernment Integration Architecture - Standards and Technical Guidelines *(eGA/EXT/ITA/001)*

5.8. eGovernment Infrastructure Architecture - Standards and Technical Guidelines *(eGA/EXT/IRA/001)*

5.9. eGovernment Processes and Governance - Standards and Technical Guidelines *(eGA/EXT/PAG/001)*

6. DOCUMENT CONTROL

Version	Name	Comment	Date
Ver. 1.0	eGA	Creation of Document	February 2016

APPENDIX

Illustration No.1 Identity Management Authorisation Model

Broadly, identity management authentication model should be of three (3) types:

i. Silo (The most common model)

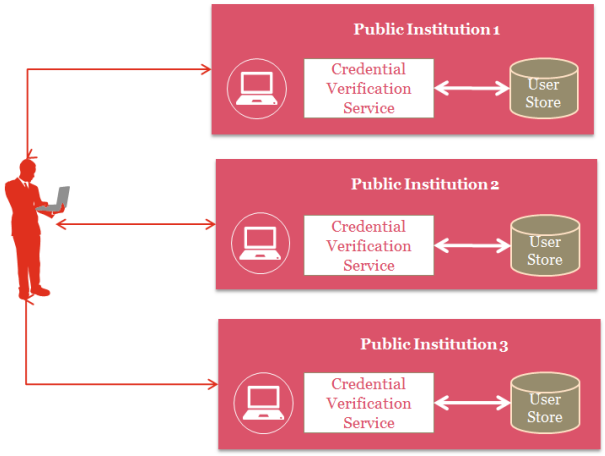

Figure III: Silo Authorization Model

a. Here the identity provider and the service provider are the same. This does not support the use of credentials across service and confined into one single service. So if there are three different services available and the user would like to subscribe to all of them then he/she might end up having three different credentials for these three services.

b. The problem with this model is the use of multiple user credentials.

c. The silo systems are not interoperable.

ii. Centralized

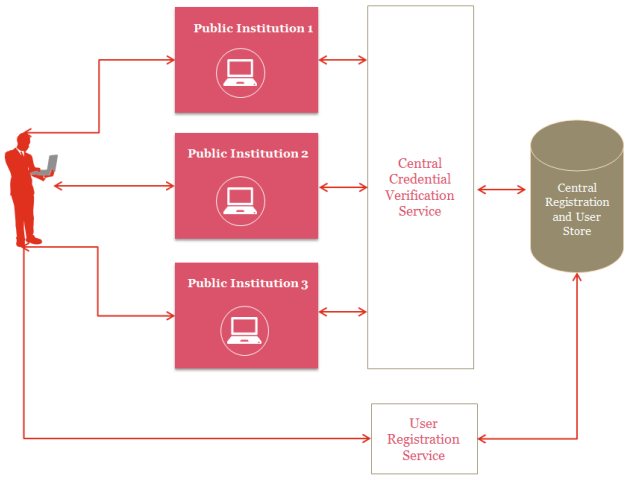

Figure IV: Centralized Authorization Model

a. Here a separate application or system acts as an exclusive user credential provider for all service providers. This architecture is very efficient in a closed environment. During registration the credential will be provided to the user by the credential provider and that will be used to access the various applications/systems.
b. This model ensures that user has a single credential to access the all the services.
c. The Central user store will also store the authorization information for the user which will be used in different application.
d. Though this model works perfectly fine with newly built system but in situations where there are existing applications with existing user bases it may be difficult to integrate the authentication components into a single platform.

iii. Federated

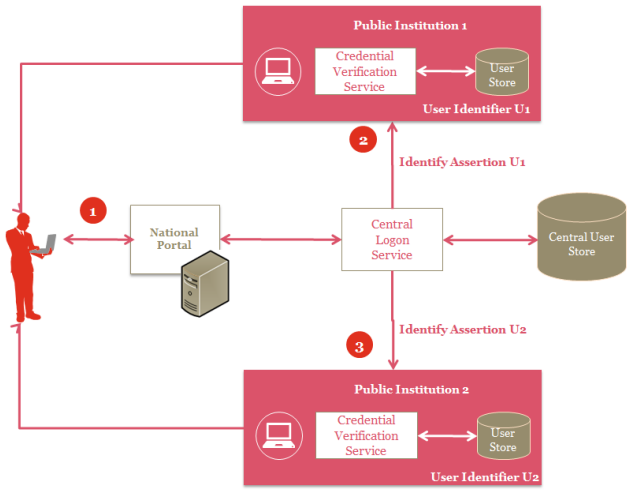

Figure V: Federated Authorization Model

a. A federated model provides a single logon service across multiple applications with a single identifier. In this model the credentials are issued by the federated Central Logon Service after a registration process. Credentials issued by this central logon service can be consumed by the other applications.