THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

e-GOVERNMENT SECURITY ARCHITECTURE – STANDARDS AND TECHNICAL GUIDELINES

Document Number eGA/EXT/ISA/001

Issued by e-Government Agency - December 2017

THE UNITED REPUBLIC OF TANZANIA

PRESIDENT'S OFFICE,
PUBLIC SERVICE MANAGEMENT

e-GOVERNMENT AGENCY

Document Title

e-Government Security Architecture – Standards and Technical Guidelines

Document Number eGA/EXT/ISA/001

APPROVAL	Name	Job Title/ Role	Signature	Date
Approved by	Dr. Jabiri Bakari	Chief Executive Officer		

Table of Contents

1.0 OVERVIEW

1.1. Introduction

The e-Government Agency (eGA) is established under the Executive Agencies Act No.30, 1997, Cap. 245 as a semi-autonomous Institution under President's Office Public Service Management. eGA is charged with the mandate of providing coordination, oversight and provision of e-Government initiatives and enforcement of e-Government standards to Public Institutions. In executing its duties, eGA shall implement and maintain coordinated government operations for Information and Communication Technology (ICT) that include the formulation of standards and guidelines to effectuate the purposes of the Agency.

To realize the vision of e-Government in Tanzania and successfully implement e-Government Strategy, it is of paramount importance that **"e-Government Standards and Guidelines"** are formulated. The e-Government Standards and Guidelines' aim is to assist in the delivery of more consistent and cohesive services to citizen and support the more cost effective delivery of ICT services by Government. A worldwide agreeable practice for conducting Government wide e-Government analysis, design, planning and implementation, using a holistic approach at all times, for the successful development and execution of e-Government Strategy is known as **"e-Government Enterprise Architecture"**. The e-Government Standards and Guidelines Structure is hereby designed to cover most requirements of e-Government Enterprise Architecture. This means that e-Government Enterprise Architecture is incorporated in "e-Government Standards & Guidelines".

Management of e-Government Standards and Guidelines requires categorisation. There are **nine categories/areas** covering all aspects of e-Government. The **eighth** area is **e-Government Security Architecture**. 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 e-Government Security Architecture is one of the methods to do that.

Security Architecture 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. The Security Architecture Standards and Technical Guidelines document is a part of Technical Reference Model as derived from the e-Government Enterprise Architecture referred in *e- Government Architecture Vision - Standards and Technical Guidelines (eGA/EXT/AVS/001).*

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. 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 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. 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;

i. **Confidentiality** for preserving authorized restrictions from access and disclosure, including means for protecting personal privacy and proprietary information;

i. **Availability** for ensuring timely and reliable access to and use of information. Availability is securely accomplished through identification, authentication, authorization and access control;

i. **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

i. **Assurance** including security administration and adherence to security and infrastructure related standards.

1.4. Scope

This document applies to all Public Institutions and involved third parties (suppliers and contractors). The Public Institution Accounting Officer (Head of Institution), Head of ICT Departments, Application Developers, Security Officers, Application Architects, Network and Infrastructure Engineers shall be responsible for ensuring the effective implementation of these specific standards and technical guidelines associated with Security Architecture within their respective Institutions.

2.0 e-GOVERNMENT SECURITY ARCHITECTURE

2.1. e-Government Security Architecture Reference Framework

e-Government Security Architecture 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:

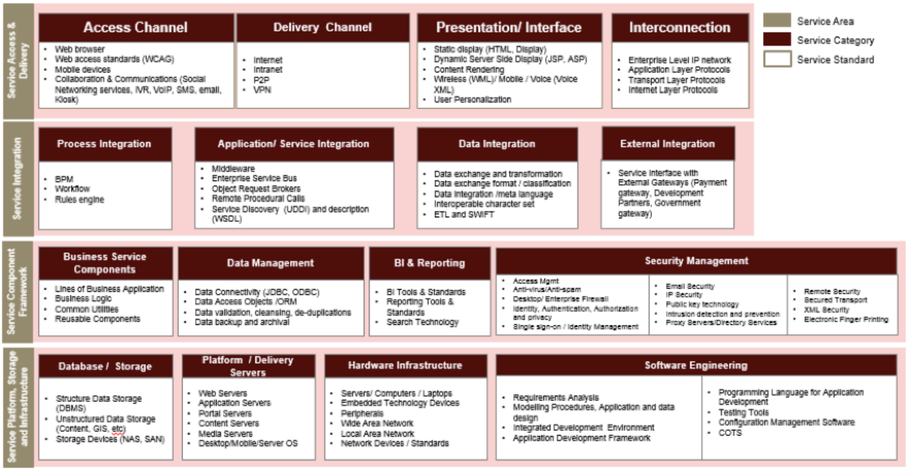
i. Service Area – Each Service Area aggregates the standards and technologies into a lower-level functional area. Each Service Area consists of multiple Service Categories and Service Standards.

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 Standards provide illustrative specifications or technologies as examples.

The following is the TRM for the Government.

Technical Reference Model



Service Access & Delivery

Access Channel
- Web browser
- Web access standards (WCAG)
- Mobile devices
- Collaboration & Communications (Social Networking services, IVR, VoIP, SMS, email, Kiosk)

Delivery Channel
- Internet
- Intranet
- P2P
- VPN

Presentation/ Interface
- Static display (HTML, Display)
- Dynamic Server Side Display (JSP, ASP)
- Content Rendering
- Wireless (WML)/ Mobile / Voice (Voice XML)
- User Personalization

Interconnection
- Enterprise Level IP network
- Application Layer Protocols
- Transport Layer Protocols
- Internet Layer Protocols

Service Integration

Process Integration
- BPM
- Workflow
- Rules engine

Application/ Service Integration
- Middleware
- Enterprise Service Bus
- Object Request Brokers
- Remote Procedural Calls
- Service Discovery (UDDI) and description (WSDL)

Data Integration
- Data exchange and transformation
- Data exchange format / classification
- Data integration /meta language
- Interoperable character set
- ETL and SWIFT

External Integration
- Service Interface with External Gateways (Payment gateway, Development Partners, Government gateway)

Service Component Framework

Business Service Components
- Lines of Business Application
- Business Logic
- Common Utilities
- Reusable Components

Data Management
- Data Connectivity (JDBC, ODBC)
- Data Access Objects /ORM
- Data validation, cleansing, de-duplications
- Data backup and archival

BI & Reporting
- BI Tools & Standards
- Reporting Tools & Standards
- Search Technology

Security Management
- Access Mgmt
- Anti-virus/Anti-spam
- Desktop/ Enterprise Firewall
- Identity, Authentication, Authorization and privacy
- Single sign-on / Identity Management

- Email Security
- IP Security
- Public key technology
- Intrusion detection and prevention
- Proxy Servers/Directory Services

- Remote Security
- Secured Transport
- XML Security
- Electronic Finger Printing

Service Platform, Storage and Infrastructure

Database / Storage
- Structure Data Storage (DBMS)
- Unstructured Data Storage (Content, GIS, etc)
- Storage Devices (NAS, SAN)

Platform / Delivery Servers
- Web Servers
- Application Servers
- Portal Servers
- Content Servers
- Media Servers
- Desktop/Mobile/Server OS

Hardware Infrastructure
- Servers/ Computers / Laptops
- Embedded Technology Devices
- Peripherals
- Wide Area Network
- Local Area Network
- Network Devices / Standards

Software Engineering
- Requirements Analysis
- Modelling Procedures, Application and data design
- Integrated Development Environment
- Application Development Framework

- Programming Language for Application Development
- Testing Tools
- Configuration Management Software
- COTS

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 be used across the security layers above are categorised and standardised across the entire Government in ten (10) Government ICT Security Domains (GISD). These domains are presented below;

1. **ICT Security Governance and Management**
2. **ICT Security Operations**
3. **Security of ICT Assets**
4. **Identity and Access Management**
5. **ICT Security Incident Management**
6. **Information Systems Continuity Management**
7. **Security of Information Systems Acquisition, Development and Maintenance**
8. **Human Resource Security**
9. **Physical and Environment Security**
10. **ICT Security Compliance and Audit**

From the Government ICT Security Domains (GISD), a security Reference Architecture Framework is derived and designed to adhere with the recommended overarching technology architecture principles (e.g. security, privacy and data protection).

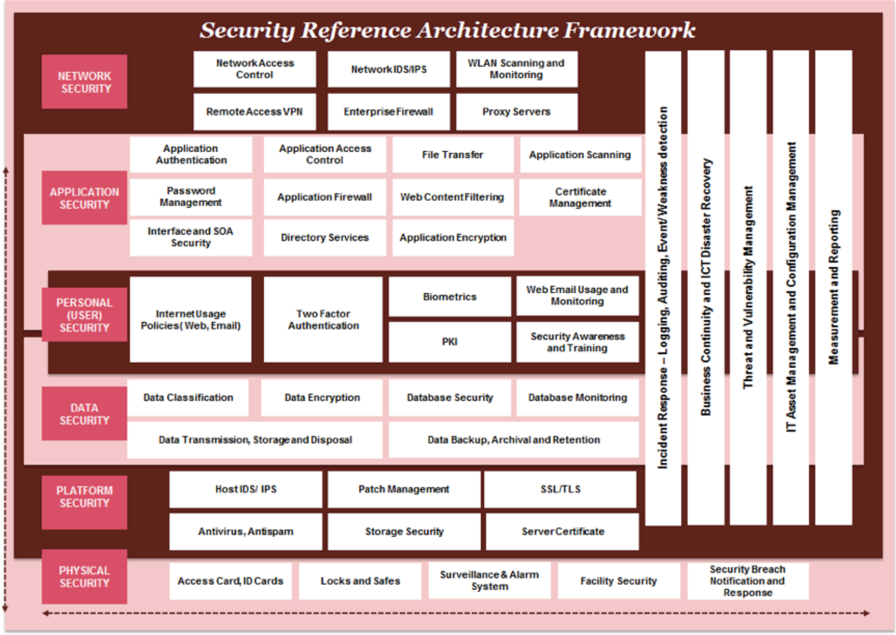

Security Reference Architecture Framework
NETWORK SECURITY
Network Access Control
Network IDS/IPS
WLAN Scanning and Monitoring
Remote Access VPN
Enterprise Firewall
Proxy Servers
APPLICATION SECURITY
Application Authentication
Application Access Control
File Transfer
Application Scanning
Password Management
Application Firewall
Web Content Filtering
Certificate Management
Interface and SOA Security
Directory Services
Application Encryption
PERSONAL (USER) SECURITY
Internet Usage Policies(Web, Email)
Two Factor Authentication
Biometrics
Web Email Usage and Monitoring
PKI
Security Awareness and Training
DATA SECURITY
Data Classification
Data Encryption
Database Security
Database Monitoring
Data Transmission, Storage and Disposal
Data Backup, Archival and Retention
PLATFORM SECURITY
Host IDS/ IPS
Patch Management
SSL/TLS
Antivirus, Antispam
Storage Security
Server Certificate
PHYSICAL SECURITY
Access Card, ID Cards
Locks and Safes
Surveillance & Alarm System
Facility Security
Security Breach Notification and Response
Incident Response – Logging, Auditing, Event/ Weakness detection
Business Continuity and ICT Disaster Recovery
Threat and Vulnerability Management
IT Asset Management and Configuration Management
Measurement and Reporting

Figure II: Security Reference Architecture Framework

The following are details of the core layers described in Figure II.

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 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. 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	Incident Response aims to address and manage any security breach or attack.
ii. Business Continuity and ICT Disaster Recovery	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.
iii. Threat and Vulnerability Management	Threat and vulnerability aims to identify risks and mitigation control in the ICT environment.
iv. ICT Asset Management	ICT Asset management is a set of business practices to manage ICT assets throughout their lifecycle.
v. Measurement and Reporting	Measurement and reporting provides information on the health check of the ICT appliances and systems.

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

Table II: 10 defined Government 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. Security of ICT Assets	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. ICT Security Compliance and Audit	Cross Pillars - Measurement and Reporting

2.2. e-Government Security Architecture Standards

2.2.1 Principles

Table III provides principles under which the e-Government Security Architecture is designed. Institutional security architecture component of enterprise architectures should also be designed basing on these principles:

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 in order to 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 security 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.

2.2.2.3 Public Institution's ICT Security posture will be evaluated from time to time using current version of Critical Security Controls for Effective Cyber Defence (From Centre for Internet Security). *Refer to Appendix B For Version 6.1 of 31st August 2016.*

2.2.4 Security of ICT Assets

2.2.4.1 For security of ICT assets 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) 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 are 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 mobilized when required.

ii. Significant incidents are reported to eGA for appropriate support to be rendered to the Public Institution 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. Resources and Disaster Recovery Plans are developed and tested.

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

iii. Continuity planning seeks 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 is aligned with Business Continuity Management for the Public Institution, where the latter exists.

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

2.2.8 Security of 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 Public 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 have to 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 ICT Security Compliance and Audit

2.2.11.1 Ensure that independent ICT security assessments 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 Ensure that records are protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislations, regulations, contractual and business requirements.

2.3 e-Government Security Architecture Technical Guidelines

Public Institutions will adhere to the following guidelines. Further references (Templated and Technical Guides) related to e-Government Security Architecture will be developed from time to time.

2.3.1 ICT Security Governance and Management

2.3.1.1 Public Institution will develop their Institutional ICT Security Policy that suit their ICT security needs as guided by *"Creation of ICT Security Policy – Technical Guide (eGA/EXT/ISA/003)"* document.

2.3.1.2 To develop Institutional ICT Security Policy, as guided by *"Creation of ICT Security Policy – Technical Guide (eGA/EXT/ISA/003)"* Public Institutions should ensure that the Policy contains Ten Government ICT Security Domains (GISD), and *"ICT Security Policy Sample (eGA/EXT/SAM/002)"* should be used.

2.3.1.3 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.

2.3.1.4 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.

2.3.1.5 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.

2.3.1.6 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.

2.3.2 ICT Security Operations

2.3.2.1 Comply with the Institutional ICT Security Policy.

2.3.2.2 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 should 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 should 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 should 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.

2.3.2.3 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

2.3.2.4 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.

2.3.2.5 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 should address the secure transfer of business information between the Public Institution and external parties.

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

2.3.2.7 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.

2.3.2.8 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.

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

2.3.2.10 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

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

2.3.2.12 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.

2.3.2.13 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.

2.3.2.14 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.

2.3.2.15 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.

2.3.2.16 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.

2.3.2.17 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.

2.3.2.18 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.

2.3.2.19 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.

2.3.2.20 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).

2.3.2.21 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.

2.3.2.22 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 should 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.

2.3.2.23 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.

2.3.2.24 Consider the following general security requirements when making use of Anti-virus:

i. Public institutions should ensure that all computers are installed with antivirus programs to prevent and remove viruses. Also, they should ensure a regular review by approved procedures.

ii. All Public Institutions must avoid using free antivirus programs available in the internet or other sources unless advised by eGA.

iii. Public institution with local area networks (LAN) should have a procedure to review antivirus programs to ensure they are regularly updated through a server and use the server to push out updates to other workstations in the LAN.

iv. Public employees who need to use mobile data storage devices from external networks/computers must run a virus scan before using the device.

2.3.3 Security of ICT Assets

2.3.3.1 The developed Institutional ICT Service Management Procedures as guided in *"Creation of ICT Service Management Procedures – Technical Guide (eGA/EXT/IRA/002)"* document, should include as integrated or a separate document ICT Asset and Configuration Management Procedures. These should clearly identify all ICT assets and the purpose of same. The information should be included in an asset register which is regularly updated.

2.3.3.2 To develop Institutional Acceptable ICT Use Policy as demonstrated in *"Acceptable ICT use Policy Template (eGA/EXT/TEM/003)"*. Public Institutions will 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).

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

2.3.3.4 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.

2.3.3.5 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.

2.3.3.6 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.

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

2.3.3.8 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, should determine which data are critical to the operations of their department.

2.3.3.9 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.

2.3.4 Identity and Access Management

2.3.4.1 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 Policies 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; and
f. provide physical or logical access controls for the isolation of sensitive applications, application data, or systems.

2.3.4.2 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 should 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.
a. 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.
b. 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.
c. 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.

2.3.4.3 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.

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

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

2.3.4.6 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.

2.3.4.7 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.

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

i. Public Institutions should 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 should 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.

2.3.4.9 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.

2.3.5 ICT Security Incident Management

2.3.5.1 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.

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

2.3.5.3 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.

2.3.6 Information Systems Continuity Management

2.3.6.1 Public Institutions will develop their Institutional **Disaster Recovery Plan** with well-established Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) of various business systems/applications and services needs as guided by *"Creation of Disaster Recovery Plan – Technical Guide (eGA/EXT/ISA/002)"* document.

2.3.6.2 To develop Institutional Disaster Recovery Plan, as guided by *"Creation Disaster Recovery Plan - Technical Guide (eGA/EXT/ISA/002)"* document, the following practices for Business Continuity Planning (BCP) and Disaster Recovery (DR), to should be considered:

i. In the event of a disaster, critical business applications must be brought back online with the least delay and restored to the most recent backup point. Develop recovery objectives for the critical services to enable recovery of ICT services after a data loss event also define what is required to meet recovery objectives and whether these goals are realistic.

ii. Outline a backup policy that governs how and when data residing on servers and other critical systems will be backed up and stored for the purpose of providing restoration capability.

iii. Formulate a backup strategy and implement three tiers of storage:
   a. Immediate/daily backups: First-tier copies must remain at hand for quick restoration of business data in case of unforeseen data loss.
   b. Periodic/Weekly backups: Second-tier copies remain nearby to supply restorations of accidentally deleted files.
   c. Long-term/Monthly: archives. Third-tier copies must be securely stored for financial and/or legal compliance.

iv. Off-site storage is a best practice to meet targets required by regulation, business continuity planning, and disaster recovery planning (DRP). Implement offsite facility for off-site storage of data either daily or weekly basis.

v. Ensure that their respective backup and restoration processes are regularly tested.

vi. Clearly identify requirements and discuss them with service providers to verify if they can be supported - economically as well as reliably. Disaster recovery plans for facilities such as the server facilities should include:
   a. Comprehensive inventory of all computer hardware, software, and support equipment.
   b. Vendor call and escalation lists.
   c. Emergency call lists for management and recovery teams.
   d. Recovery team duties and responsibilities.
   e. Equipment room floor grid diagrams.
   f. Copies of contracts and maintenance agreements.
   g. Procedures for securing the damaged site.
   h. Procedures for restoring or replacing support systems, such as power, air conditioning, and uninterrupted power supply.

2.3.7 Security of Information Systems Acquisition, Development and Maintenance

2.3.7.1 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.

2.3.7.2 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

2.3.7.3 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.

2.3.7.4 Public Institutions adopting mobile technologies such as BYOD should deploy mobile devices management for managing secure operations and monitoring of mobile devices which hold the distribution of corporate application and data.

2.3.8 Human Resource Security

2.3.8.1 Security awareness and training - An information security awareness programme should 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 should 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 should take place periodically.

2.3.9 Physical and Environment Security

2.3.9.1 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.

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

2.3.9.3 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.

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

2.3.9.5 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.

2.3.10 ICT Security Compliance and Audit

2.3.10.1 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.

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

3. IMPLEMENTATION, REVIEW AND ENFORCEMENT

3.1 This document takes effect from December, 2017.

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

3.3 Any exceptions to compliance with this document should be approved in writing by Chief Executive Officer (CEO) of e-Government Agency.

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. e-Government Guideline 2017 by President's Office – Public Service Management (PO-PSM)

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

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

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

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

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

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

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

5.9. e-Government Architecture 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
Ver. 1.1	eGA	Alignment with e-Government Guideline 2017	December 2017

APPENDIX

A. Illustration No.1 Identity Management Authorisation Model

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

i. Silo (The most common model)

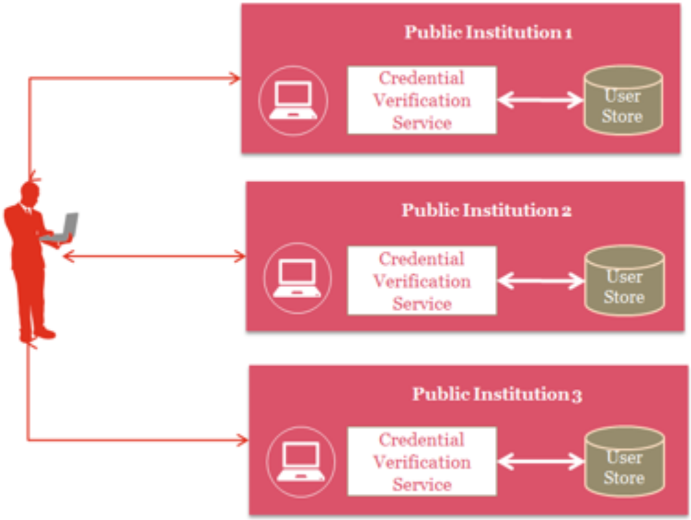

Public Institution 1
Credential Verification Service
User Store
Public Institution 2
Credential Verification Service
User Store
Public Institution 3
Credential Verification Service
User Store

Figure AI: 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

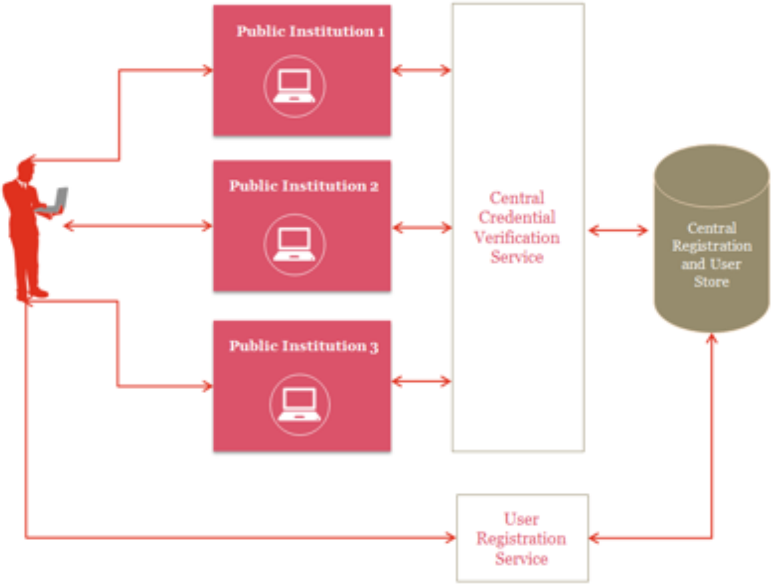

Public Institution 1
Public Institution 2
Public Institution 3
Central Credential Verification Service
Central Registration and User Store
User Registration Service

Figure AII: 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

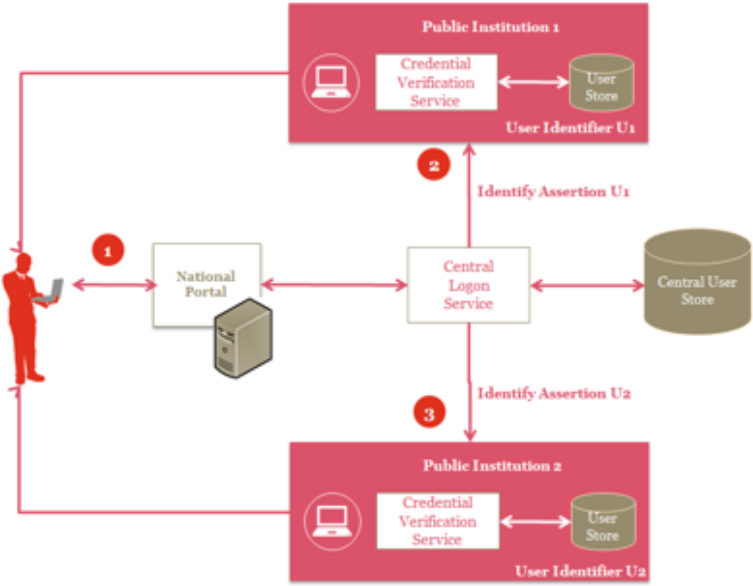


Figure AIII: Federated Authorization Model

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.

B. Critical Security Controls for Effective Cyber Defense

Table A1: The Center for Internet Security Critical Security Controls for Effective Cyber Defense - Version 6.1 released on August 31, 2016

Family	Control	Control Description
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices		
System	1.1	Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.
System	1.2	If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems.
System	1.3	Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network.
System	1.4	Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

System	1.5	Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems.
System	1.6	Use client certificates to validate and authenticate systems prior to connecting to the private network.
Critical Security Control #2: Inventory of Authorized and Unauthorized Software		
System	2.1	Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified.
System	2.2	Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.
System	2.3	Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software are tracked from a single location.
System	2.4	Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment.

Critical Security Control #3: Secure Configurations for Hardware and Software		
System	3.1	Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.
System	3.2	Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization.
System	3.3	Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.
System	3.4	Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as SSL, TLS or IPSEC.
System	3.5	Use file integrity checking tools to ensure that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered. The reporting system should: have the ability to account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration

		changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by attackers or additional files inappropriately added during batch distribution processes).
System	3.6	Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible use tools compliant with the Security Content Automation Protocol (SCAP) in order to streamline reporting and integration.
System	3.7	Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis.
Critical Security Control #4: Continuous Vulnerability Assessment and Remediation		
System	4.1	Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the

		Common Configuration Enumeration Project).
System	4.2	Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable.
System	4.3	Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user.
System	4.4	Subscribe to vulnerability intelligence services in order to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities.
System	4.5	Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.
System	4.6	Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans.
System	4.7	Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed either by patching, implementing a compensating control, or documenting

		and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that were previously accepted, or if conditions have changed, increasing the risk.
System	4.8	Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level.
Critical Security Control #5: Controlled Use of Administrative Privileges		
System	5.1	Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.
System	5.2	Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive.
System	5.3	Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration-level accounts.
System	5.4	Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system.
System	5.5	Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account.

System	5.6	Use multifactor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.
System	5.7	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
System	5.8	Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems.
System	5.9	Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.
Critical Security Control #6: Maintenance, Monitoring, and Analysis of Audit Logs		
System	6.1	Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent.
System	6.2	Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

System	6.3	Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis.
System	6.4	Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings.
System	6.5	Configure network boundary devices, including firewalls, network-based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device.
System	6.6	Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.
Critical Security Control #7: Email and Web Browser Protections		
System	7.1	Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes.
System	7.2	Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains.
System	7.3	Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities.

System	7.4	Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.
System	7.5	Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.
System	7.6	The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not.
System	7.7	To lower the chance of spoofed e-mail messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver-side verification in mail servers.
System	7.8	Scan and block all e-mail attachments entering the organization's e-mail gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the e-mail is placed in the user's inbox. This includes e-mail content filtering and web content filtering.
Critical Security Control #8: Malware Defenses		
System	8.1	Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

System	8.2	Employ anti-malware software that offers a centralized infrastructure that compiles information on file reputations or have administrators manually push updates to all machines. After applying an update, automated systems should verify that each system has received its signature update.
System	8.3	Limit use of external devices to those with an approved, documented business need. Monitor for use and attempted use of external devices. Configure laptops, workstations, and servers so that they will not auto-run content from removable media, like USB tokens (i.e., "thumb drives"), USB hard drives, CDs/DVDs, FireWire devices, external serial advanced technology attachment devices, and mounted network shares. Configure systems so that they automatically conduct an anti-malware scan of removable media when inserted.
System	8.4	Enable anti-exploitation features such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), virtualization/containerization, etc. For increased protection, deploy capabilities such as Enhanced Mitigation Experience Toolkit (EMET) that can be configured to apply these protections to a broader set of applications and executables.
System	8.5	Use network-based anti-malware tools to identify executables in all network traffic and use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint.
System	8.6	Enable domain name system (DNS) query logging to detect hostname lookup for known malicious C2 domains.
Critical Security Control #9: Limitation and Control of Network Ports, Protocols, and Services		
System	9.1	Ensure that only ports, protocols, and services with validated business needs are running on each system.
System	9.2	Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

System	9.3	Perform automated port scans on a regular basis against all key servers and compared to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.
System	9.4	Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address.
System	9.5	Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers.
System	9.6	Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated.
Critical Security Control #10: Data Recovery Capability		
System	10.1	Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.
System	10.2	Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.
System	10.3	Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

System	10.4	Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations.
Critical Security Control #11: Secure Configurations for Network Devices		
Network	11.1	Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.
Network	11.2	All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.
Network	11.3	Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.
Network	11.4	Manage network devices using two-factor authentication and encrypted sessions.
Network	11.5	Install the latest stable version of any security-related updates on all network devices.
Network	11.6	Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Network	11.7	Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.
Critical Security Control #12: Boundary Defense		
Network	12.1	Deny communications with (or limit data flow to) known malicious IP addresses (black lists), or limit access only to trusted sites (whitelists). Tests can be periodically carried out by sending packets from bogon source IP addresses (non-routable or otherwise unused IP addresses) into the network to verify that they are not transmitted through network perimeters. Lists of bogon addresses are publicly available on the Internet from various sources, and indicate a series of IP addresses that should not be used for legitimate traffic traversing the Internet.
Network	12.2	On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.
Network	12.3	Deploy network-based IDS sensors on Internet and extranet DMZ systems and networks that look for unusual attack mechanisms and detect compromise of these systems. These network-based IDS sensors may detect attacks through the use of signatures, network behavior analysis, or other mechanisms to analyze traffic.
Network	12.4	Network-based IPS devices should be deployed to complement IDS by blocking known bad signatures or the behavior of potential attacks. As attacks become automated, methods such as IDS typically delay the amount of time it takes for someone to react to an attack. A properly configured network-based IPS can provide automation to block bad traffic. When evaluating network-based IPS products, include

		those using techniques other than signature-based detection (such as virtual machine or sandbox-based approaches) for consideration.
Network	12.5	Design and implement network perimeters so that all outgoing network traffic to the Internet must pass through at least one application layer filtering proxy server. The proxy should support decrypting network traffic, logging individual TCP sessions, blocking specific URLs, domain names, and IP addresses to implement a black list, and applying whitelists of allowed sites that can be accessed through the proxy while blocking all other sites. Organizations should force outbound traffic to the Internet through an authenticated proxy server on the enterprise perimeter.
Network	12.6	Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.
Network	12.7	All enterprise devices remotely logging into the internal network should be managed by the enterprise, with remote control of their configuration, installed software, and patch levels. For third-party devices (e.g., subcontractors/ vendors), publish minimum security standards for access to the enterprise network and perform a security scan before allowing access.
Network	12.8	Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.
Network	12.9	Deploy NetFlow collection and analysis to DMZ network flows to detect anomalous activity.
Network	12.10	To help identify covert channels exfiltrating data through a firewall, configure the built-in firewall session tracking mechanisms included in many commercial firewalls to identify TCP sessions that last an unusually long time for the given organization and firewall device, alerting personnel about the source and destination addresses associated with these long sessions.

Critical Security Control #13: Data Protection		
Network	13.1	Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity controls.
Network	13.2	Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.
Network	13.3	Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across network boundaries and block such transfers while alerting information security personnel.
Network	13.4	Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information.
Network	13.5	If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.
Network	13.6	Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them.
Network	13.7	Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations be able to detect

		rogue connections, terminate the connection, and remediate the infected system.
Network	13.8	Block access to known file transfer and e-mail exfiltration websites.
Network	13.9	Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop system, the ACLs are no longer enforced and the users can send the data to whomever they want.
Critical Security Control #14: Controlled Access Based on the Need to Know		
Application	14.1	Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities.
Application	14.2	All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted.
Application	14.3	All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to directly communicate with other devices on the subnet and limit an attackers ability to laterally move to compromise neighboring systems.
Application	14.4	All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.
Application	14.5	Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not

		integrated into the operating system, in order to access the information.
Application	14.6	Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data.
Application	14.7	Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed.
Critical Security Control #15: Wireless Access Control		
Network	15.1	Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile.
Network	15.2	Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated.
Network	15.3	Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network.
Network	15.4	Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface).
Network	15.5	Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least

		Wi-Fi Protected Access 2 (WPA2) protection.
Network	15.6	Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication.
Network	15.7	Disable peer-to-peer wireless network capabilities on wireless clients.
Network	15.8	Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.
Network	15.9	Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly.
Critical Security Control #16: Account Monitoring and Control		
Application	16.1	Review all system accounts and disable any account that cannot be associated with a business process and owner.
Application	16.2	Ensure that all accounts have an expiration date that is monitored and enforced.
Application	16.3	Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.
Application	16.4	Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity.
Application	16.5	Configure screen locks on systems to limit access to unattended workstations.
Application	16.6	Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active

		employees and contractors with each account belonging to their managed staff. Security or system administrators should then disable accounts that are not assigned to valid workforce members.
Application	16.7	Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time.
Application	16.8	Monitor attempts to access deactivated accounts through audit logging.
Application	16.9	Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well.
Application	16.10	Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.
Application	16.11	Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.
Application	16.12	Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).
Application	16.13	Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.
Application	16.14	Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Critical Security Control #17: Security Skills Assessment and Appropriate Training to Fill Gaps		
Application	17.1	Perform gap analysis to see which skills employees need and which behaviors employees are not adhering to, using this information to build a baseline training and awareness roadmap for all employees.
Application	17.2	Deliver training to fill the skills gap. If possible, use more senior staff to deliver the training. A second option is to have outside teachers provide training onsite so the examples used will be directly relevant. If you have small numbers of people to train, use training conferences or online training to fill the gaps.
Application	17.3	Implement an security awareness program that (1) focuses only on the methods commonly used in intrusions that can be blocked through individual action, (2) is delivered in short online modules convenient for employees (3) is updated frequently (at least annually) to represent the latest attack techniques, (4) is mandated for completion by all employees at least annually, and (5) is reliably monitored for employee completion.
Application	17.4	Validate and improve awareness levels through periodic tests to see whether employees will click on a link from suspicious e-mail or provide sensitive information on the telephone without following appropriate procedures for authenticating a caller; targeted training should be provided to those who fall victim to the exercise.
Application	17.5	Use security skills assessments for each of the mission-critical roles to identify skills gaps. Use hands-on, real-world examples to measure mastery. If you do not have such assessments, use one of the available online competitions that simulate real-world scenarios for each of the identified jobs in order to measure skills mastery.
Critical Security Control #18: Application Software Security		
Application	18.1	For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches

		and vendor security recommendations.
Application	18.2	Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed.
Application	18.3	For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats.
Application	18.4	Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. In particular, input validation and output encoding routines of application software should be reviewed and tested.
Application	18.5	Do not display system error messages to end-users (output sanitization).
Application	18.6	Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments.
Application	18.7	For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.
Application	18.8	Ensure that all software development personnel receive training in writing secure code for their specific development environment.

Application	18.9	For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in the deployed software, or accessible in the production environment.
Critical Security Control #19: Incident Response and Management		
Application	19.1	Ensure that there are written incident response procedures that include a definition of personnel roles for handling incidents. The procedures should define the phases of incident handling.
Application	19.2	Assign job titles and duties for handling computer and network incidents to specific individuals.
Application	19.3	Define management personnel who will support the incident handling process by acting in key decision-making roles.
Application	19.4	Devise organization-wide standards for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting should also include notifying the appropriate Community Emergency Response Team in accordance with all legal or regulatory requirements for involving that organization in computer incidents.
Application	19.5	Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an e-mail address of **security@organization.com** or have a web page **http://organization.com/security).**
Application	19.6	Publish information for all personnel, including employees and contractors, regarding reporting computer anomalies and incidents to the incident handling team. Such information should be included in routine employee awareness activities.
Application	19.7	Conduct periodic incident scenario sessions for personnel associated with the incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the incident handling team.

Critical Security Control #20: Penetration Tests and Red Team Exercises		
Application	20.1	Conduct regular external and internal penetration tests to identify vulnerabilities and attack vectors that can be used to exploit enterprise systems successfully. Penetration testing should occur from outside the network perimeter (i.e., the Internet or wireless frequencies around an organization) as well as from within its boundaries (i.e., on the internal network) to simulate both outsider and insider attacks.
Application	20.2	Any user or system accounts used to perform penetration testing should be controlled and monitored to make sure they are only being used for legitimate purposes, and are removed or restored to normal function after testing is over.
Application	20.3	Perform periodic Red Team exercises to test organizational readiness to identify and stop attacks or to respond quickly and effectively.
Application	20.4	Include tests for the presence of unprotected system information and artifacts that would be useful to attackers, including network diagrams, configuration files, older penetration test reports, e-mails or documents containing passwords or other information critical to system operation.
Application	20.5	Plan clear goals of the penetration test itself with blended attacks in mind, identifying the goal machine or target asset. Many APT-style attacks deploy multiple vectors—often social engineering combined with web or network exploitation. Red Team manual or automated testing that captures pivoted and multi-vector attacks offers a more realistic assessment of security posture and risk to critical assets.
Application	20.6	Use vulnerability scanning and penetration testing tools in concert. The results of vulnerability scanning assessments should be used as a starting point to guide and focus penetration testing efforts.
Application	20.7	Wherever possible, ensure that Red Teams results are documented using open, machine-readable standards (e.g., SCAP). Devise a scoring method for determining the results of Red Team exercises so that results can be compared over time.

Application	20.8	Create a test bed that mimics a production environment for specific penetration tests and Red Team attacks against elements that are not typically tested in production, such as attacks against supervisory control and data acquisition and other control systems.

Issued by e-Government Agency - December 2017