NATIONAL CYBERSECURITY POLICY/STRATEGY IMPLEMENTATION GUIDELINES

FOR

MINISTRIES, DEPARTMENTS & AGENCIES (MDAs)

&

PRIVATE ICT ORGANZATIONS

AUGUST 2019

TABLE OF CONTENTS

1.0 PREAMBLE

These guidelines are issued to ensure coordinated and standardized actionable processes in the handling of cybersecurity issues in the country. The need for the development of the Guidelines arose from the fact that full traction of the National Cybersecurity Policy and Strategy had not been fully realized.

The purposes of these guidelines are to ensure:

a) that IT Firms and MDAs duly adhere to the Governments direction in cybersecurity matters;

b) cybersecurity infractions have given Nigeria and Nigerians a deplorable image globally and should be treated as a national issue;

c) that the technology and services procured are suitable for the country from the point of view of security and the environment, among others;

d) the central coordination included in the Policy/Strategy are fully realized, for ensuring national security in cyberspace;

e) that the digital economy cannot thrive if trust in cyberspace and eCommerce and other interdependencies are trusted and supported by all Nigerians; and f) that the technology being implemented is up-to-date.

2.0 AUTHORITY

These guidelines are issued pursuant to:

a) Chapter 3.1 of the National Information Technology Policy of 2000 which states that the nation shall use IT as the major driving force to re-engineer and rapidly transform governance to interface with the needs of its citizenry by establishing transparent 'Government Wide Information System' at all levels.

b) Section 6 of the NITDA Act 2007 which mandates the Agency to do the following:

i. create a framework for the planning, research, development, standardization, application, coordination, monitoring, evaluation and regulation of Information Technology practices, activities and systems in Nigeria and all matters related thereto and for that purpose…;

ii. develop guidelines for electronic governance and monitor the use of electronic data interchange and other forms of electronic communication transactions as an alternative to paper-based methods in government, commerce, education, the private and public sectors, labour, and other fields, where the use of electronic communication may improve the exchange of data and information;

iii. render advisory services in all information technology matters to the public and private sectors;

iv. perform such other duties, which in the opinion of the Agency are necessary or expedient to ensure the efficient performance of the functions of the Agency under this Act.

3.0 SHORT TITLE AND COMMENCEMENT

This Guidelines shall be cited as ‘National Cybersecurity Policy/Strategy Implementation Guidelines’ and shall come into effect when it is signed by the Director General of NITDA.

4.0 DEFINITIONS

ARCHITECTURE

This details the structure and behavior of the technology infrastructure. Covers the client and server nodes of the hardware configuration, the infrastructure applications that run on them, the infrastructure services they offer to applications, the protocols and networks that connect applications and nodes. Assurance Part of corporate governance in which management provides accurate and current information to their stakeholders about the efficiency and effectiveness of its policies and operations, and the status of its compliance with statutory obligations.

ARTIFACTS

Critical Infrastructure: a term used by governments to describe assets that are essential for the functioning of a society and economy.

Cyber Conflict: The carrying out of large-scale, economic, political and commercial conflicts through cyberspace.

CYBERCRIME

Cybercrime is criminal activity undertaken using computers and the Internet. Cyberspace The electronic medium of computer networks, in which online communication takes place Cybersecurity Cyber security includes information and technical security applied to hardware, software and systems that make up networks.

CYBER RISK

The specific risks associated with the use of computers, information technology and the Internet.

CYBERTHREAT

The possibility of a malicious attempt to damage or disrupt a computer network or system.

CYBER-TERRORISM

The intentional use of computer, networks, and public internet to cause destruction and harm.

Data Protection: legal obligations around control over processing, access and use of personally identifiable information.

DATA RETENTION

Data retention defines the policies of persistent data and records management for meeting legal and business data archival requirements.

ECONOMIC ESPIONAGE

A form of espionage conducted for commercial purposes instead of purely national security exposure. The quantified potential for loss that might occur as a result of some activity Hacktivists Individuals or organizations who use computers and computer networks to promote political ends, chiefly free speech, human rights, and information ethics. They carry these out under the premise that proper use of technology can produce results like those of conventional acts of protest, activism, and civil disobedience.

LAWFUL INTERCEPTION

Obtaining communications network data pursuant to lawful authority for the purpose of analysis or evidence.

INCIDENT MANAGEMENT

The activities of an organization to identify, analyses, and correct hazards to prevent a future re-occurrence.

MILITARY ESPIONAGE

Spying on potential or actual enemies primarily for military purposes. Privacy: The right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed.

VISION 20:2020

Plan to position Nigeria as one of the top 20 economies in the world by the year 2020.

VULNERABILITY

A weakness which allows an attacker to reduce a system's information assurance.

5.0 ABBREVIATIONS

3PC	Public-Private Partnership for Cyber Security
CAM	Child Abuse Material
CCLR	Cybercrime Legislative Review Committee
CEMS	Cyber Emergency Monitoring System
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CIIPR	Critical Information Infrastructure Protection and Resilience
CIP	Critical Infrastructure Protection
CIPMA	Critical Infrastructure Program for Modeling and Analysis
COAEPS	Child Online Abuse and Exploitation Protection Strategy
COBIT	Control Objectives for Information and Related Technology
CSIRT	Computer Security Incident Response Team
CTM	Countermeasures Technical Mechanisms
ESP	Email Service Provider
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
IEEE	Institute of Electrical and Electronic Engineers
IGF	Internet Governance Forum
INTERPOL	International Police
ISP	Internet Service Provider
ITIL	Information Technology Infrastructure Library
ITU	International Telecommunication Union
KGI	Key Gold Indicator
KPI Key	Performance Indicators
LEA	Law Enforcement Agency
MINT	Malaysia, Indonesia, Nigeria, Turkey
NCC	Nigerian Communications Commission
NCCC	National Cybersecurity Coordinating Center
NCII	National Critical Information Infrastructure
NCIIP	National Critical Information Protection Plan
NCSS	National Cyber Security Strategy
NgCERT	Nigeria Computer Emergency Team
NIOC	Nigerian Institute of National Security
NIRP	National Incident Response Plan
NISI	National Internet Safety Initiative
NITDA	National Information Technology Development Agency
NTWG	National Technical Working Group
ONSA	Office of the National Security Advisor
PMBOK	Project Management Body of Knowledge
PPP	Public-Private Partnership
PPPMF	Public-Private Partnership Management Framework
PPPMS	Public-Private Partnership Management Strategy
PRINCE2	Project Management in a Controlled Environment
SPV	Special Purpose Vehicle
SSP	Sector Specific Plan
TISN	Trust Information Sharing Network

TOGAF	The Open Group Architecture Framework
USD	United States Dollar
UNICEF	United Nations Children's Fund
VNT	Virtual National Task Force

6.0 INTRODUCTION

We live in a hyper-connected world that is increasingly becoming more connected on the Internet and its associated information networks and operating space, commonly referred to as the cyberspace.

As at today, the Internet, the network of networks, provides information sharing and communication systems to more than 7 billion users and this number is growing across the globe.

Securing the nation's Information Security Assets, Infrastructures, networks, and systems is one of the most important challenges we face as a nation. As a result, the National Information Technology Development Agency (NITDA) is saddled with the responsibility of managing and regulating the nation's technology, by bringing significant resources to ensure cybersecurity remains a top priority.

This includes strengthening government-wide processes for developing, implementing, and institutionalizing best practices; developing and retaining the cybersecurity workforce; and working with public and private sector, research and development communities to leverage the best of existing, new, and emerging technologies.

As cyberspace becomes a driving force for productivity and development, which makes the protection of critical information infrastructure a national security responsibility requiring government, public and private sector to collaborate and synergize. The nation depends on this critical information infrastructure (CII) for essential service delivery, and as the CII becomes a target of cybercrimes, as experienced globally, all efforts and synergy are required to avert a national calamity arising from cyberattacks. For this reason, NITDA, by this Guideline, in collaboration with all relevant Stakeholders, has reviewed the National Cybersecurity Policy/Strategy, for optimal effectiveness.

The Guidelines assigns roles and responsibilities to all critical stakeholders, MDAs, Private IT Companies, players of all other sectors of the economy, civil society groups, the general public and other residents of Nigeria, to safeguard itself and associated infrastructure, for an aggregate national resiliency. NITDA's role in ensuring compliance is highlighted in all the sections of the guidelines.

1 NATIONAL CYBERSECURITY GOVERNANCE, COORDINATION & ASSURANCE MECHANISM

OBJECTIVE

The objective of this section is to establish and give guidance on the implementation of national cyber security governance and information security assurance.

ROLES AND RESPONSIBILITIES OF NITDA

Coordinate the management and implementation of national cybersecurity initiatives and all related programs as provided for in the National Cybersecurity Strategy and in line with extant laws.

Monitor and evaluate Nigeria's cybersecurity maturity and compliance with the National Cybersecurity Strategy, Cybercrime Act, 2015 as well as guidelines, standards and other regulatory requirements.

Develop comprehensive Key Performance Indicators (KPI) to measure progress and effectiveness of national efforts to combat cyber threats and countermeasures.

ROLES AND RESPONSIBILITIES OF MDAs and PRIVATE ICT ORGANIZATIONS

MDA'S/PRIVATE ICT ORGANIZATIONS shall:

i. Ensure that the Directors General, MD/CEO and Senior management of all organizations agree to sponsor, provide the required support and resources for the implementation of cyber security programs. Hence an annual budget must exist to organize cybersecurity programs in each of these organizations.

ii. Ensure that cybersecurity program becomes an integral part of corporate governance which rests with the Board of Directors of all MDAs & Private ICT Organizations.

iii. Ensure all MDAs and Private ICT Organizations have a designated Chief Information Security Officer (CISO) as a staff of the Agency/Organization who is a member of the senior management and has the requisite skills & qualifications.

iv. Ensure the Implementation of Information security management system (ISO 27001) and Cyber Security Program in all applicable MDAs & Private ICT Organizations (see the Roadmap addendum).

v. Ensure monitoring and evaluation of cybersecurity maturity, coordinate investigation, prosecution and enforce compliance by conducting periodic compliance assessments.

THE RESPONSIBILITIES OF THE BOARD OF DIRECTORS

i. The Board of Directors through its committees shall have overall responsibility for the MDAs & Private ICT Organizations ISMS & cybersecurity programs. It shall provide leadership and direction for effective conduct of the processes. The Board shall ensure that cybersecurity governance is integrated into the organizational structure and relevant processes.

ii. The Board shall ensure that the ISMS and cyber security processes are conducted in line with business requirements, applicable laws and regulations while ensuring security expectations are defined and met across all MDAs & Private ICT organizations. Furthermore, the Board shall hold Senior Management responsible for central oversight, assignment of responsibility, effectiveness of the cybersecurity processes and shall ensure that the audit function is independent, effective and comprehensive.

iii. The Board shall be responsible for all ISMS and cyber security governance documents such as cybersecurity strategy, framework and policies and ensure alignment with the overall institutional goals and objectives to ensure effectiveness.

iv. The Board of all MDAs & Private shall appoint or designate a qualified individual as the "Chief Information Security Officer" (CISO) who shall be responsible for overseeing and the implementation of ISMS/cyber security program.

v. The Board shall, on a quarterly basis receive and review reports submitted by Senior Management. The report shall detail the overall status of the ISMS & cyber security program to ensure that Board approved risk thresholds relating to ISMS & cyber security are being adhered to.

THE RESPONSIBILITIES OF SENIOR MANAGEMENT

i. Senior Management shall be responsible for the implementation of the Board-approved ISMS & cyber security policies, standards and the delineation of cybersecurity responsibilities.

ii. Senior Management shall provide periodic reports (at a minimum quarterly); to the Board on the overall status of the ISMS & cyber security program of MDAs & Private.

THE RESPONSIBILITIES OF THE CHIEF INFORMATION SECURITY OFFICER (CISO) ARE DETAILED BELOW:

i. The CISO shall be responsible for the day-to-day ISMS & cyber security management activities and the mitigation of cybersecurity risks in all MDAs & Private ICT.

ii. The CISO shall focus on the MDAs & Private Organization-wide ISMS & cyber security risk rather than IT operations security risk and shall also be responsible for the implementation of the cybersecurity strategy as approved by the Board.

iii. The CISO shall possess adequate authority, experience; independence and status within the MDAs & Private organizations to enable him/her function properly.

iv. The CISO should not report to the CIO/Head of Information Technology (IT) operations and to ensure segregation of duty, the two offices shall report to separate individuals.

v. The CISO shall possess educational and work experience requirements in accordance with industry best practices with professional certification required. In addition, the CISO shall possess any or a combination of Masters in Cyber/Information Security, Certified Information Systems Security Professional (CISSP) OR Certified Information Security Manager (CISM) certifications with in-depth experience in Information Technology

THE INFORMATION SECURITY STEERING COMMITTEE (ISSC):

i. Applicable MDAs & Private ICT Organizations shall establish an information security steering Committee that shall be responsible for the governance of the ISMS & cyber security program. The steering Committee shall consist of senior representatives of relevant departments within the MDAs & Private organization.

ii. The roles, responsibilities, scope and activities of the information security steering Committee shall be clearly defined.

THE OBJECTIVES OF THE COMMITTEE SHALL INCLUDE:

i. Ensuring that organizations security policies and processes align with the business objectives.

ii. Evaluating, approving, and sponsoring institution-wide security investment; Enforcing the implementation of policies for investment prioritization and security risk management; and Providing strategic direction and cybersecurity governance for the MDA's & Private ICT Organizations.

2 LEGAL AND REGULATORY FRAMEWORK

OBJECTIVE

The objective of this section is to establish and give guidance on the Implementation of national legal and regulatory framework.

ROLES AND RESPONSIBILITIES OF NITDA

i. To develop and implement comprehensive cybercrime legislations, policy and strategy that are nationally adoptable, regionally and globally relevant in the context of securing the nation's cyberspace.

ii. To ensure Nigeria, in Collaboration with the ONSA signing relevant international treaties and conventions on cybercrime and cybersecurity

ROLES AND RESPONSIBILITIES OF MDAs and PRIVATE ICT ORGANIZATIONS

MDAs and PRIVATE ICT ORGANIZATIONS SHALL:

i. Ensure the Board and Senior Management complies with relevant statutes and regulations such as the Nigerian Cybercrimes (Prohibition, Prevention etc.) Act, 2015 and all NITDA, National Information Technology Agency directives to avoid breaches of legal, statutory, regulatory obligations related to cybersecurity and of any security requirements.

ii. Ensure the establishment of appropriate processes and procedures for the purpose of monitoring compliance with this National Cybersecurity implementation guideline and other regulatory standards.

3 NATIONAL CYBER INCIDENT MANAGEMENT & PERFORMANCE MEASUREMENT

OBJECTIVE

The objective of this section is to establish and give guidance on the Implementation of national cyber incident management and performance measurement.

ROLES AND RESPONSIBILITIES OF NITDA

i. To provide real-time situational awareness through monitoring, evaluation and analysis of cyber-threats as well as providing timely response to cybersecurity incidents relating to the Nigerian cyberspace.

ii. To develop and administer a National Cyber Incident Response Plan outlining comprehensive cyber-threat counter measures, coordinating timely and proactive incidents management across all sectors of the economy.

iii. To facilitate periodic review of cyber threats, counter-measures, standards, guidelines and best practices for sector-based CSIRTs in line with national security imperatives (To develop a Cyber Threat Review Template)

iv. Develop Policy template to capture NITDA's recommendation according to best standard for all stakeholders

ROLES AND RESPONSIBILITY OF MDAs and PRIVATE ICT ORGANIZATIONS

MDA'S/PRIVATE ICT ORGANIZATIONS SHALL:

i. Where applicable have a Security Information and Event Management (SIEM) solution that aggregates data from various security feeds to provide real-time analysis of security alerts.

ii. Where applicable, ensure the Cyber Security /Information Security Team managing the Security Information and Event Management (SIEM) will be able to perform prompt Remediation service.

iii. Develop Disaster Recovery and Business Continuity plan documents (DR/BCP) with the Business (stakeholders) to ensure they are adequate and effective to support cybersecurity resilience.

iv. Develop an Incident Response (IR) policy and an Incident Response reporting Template.

THE IR POLICY SHALL STIPULATE:

i. The creation of a cyber-incident response plan approved by the Board of Directors
ii. Senior management and business process owner's definition of an Acceptable Interruption Window (AIW) for all categories of cyber-incidents; and performance metric at each stage of the Incident Response process.
iii. The establishment of a dedicated team whose focus shall be on detecting and responding to cyber-incidents.
iv. Adequate and continuous training of the Incidence Response Team on how to respond, report cyber-incidents, and conduct trend analysis to thwart future occurrence.
v. Conducting cybersecurity drills based on the approved cyber-incident response plan and test schedule to ascertain its viability, effectiveness and efficiency.
vi. Appropriate chain of custody when collecting, analyzing and reporting cyber-incidents in a manner that is legally admissible.
vii. All crisis information shall be communicated and shared with the management and ngCERT.

4 CRITICAL NATIONAL INFORMATION INFRASTRUCTURE (CNII) PROTECTION & RESILIENCE

OBJECTIVE

The objective of this section is to establish and give guidance on the Implementation of national Information infrastructure protection and resilience.

ROLES AND RESPONSIBILITIES OF NITDA

i. To carryout comprehensive identification, classification, risk assessment on Critical Information Infrastructure Protection (CIIP) to reduce their vulnerabilities and risk exposure to cyber incidents.

ii. Establish baseline for a regular Critical National Information Infrastructure (CNII) Threat Barometer & Vulnerabilities Assessment. Commence Annual National Preparedness Report on Critical Information Infrastructure security and resilience.

iii. The Risk Management Framework shall cover the four basic activities below

    Risk measurement

    Risk mitigation/Risk treatment

iv. monitoring and reporting

ROLES AND RESPONSIBILITIES OF MDAs and PRIVATE ICT ORGANIZATIONS

MDAs and PRIVATE ICT ORGANIZATIONS SHALL:

Confirm from ONSA if it belongs to those designated as CNII, or assess itself with criteria such as, do our core services:

a) Control or involve a reasonable national interconnected service usage,
b) Involve automated control of utilities services such as in transportation, power, etc
c) Financial and national data processing/transmitting capabilities/ function, etc;
d) Render critical IT interconnectivity service, etc

When designated CNII, the MDA/organization should:

i. Conduct periodic Risk assessment to evaluate the economic and security value of its activities (as prescribed in its risk treatment plan) measurement, monitor /treatment and reporting such to its management and quarterly to committee of ONSA/NITDA for certification.

ii. Ensure applicable MDAs & Private ICT Organizations maintain an up-to-date inventory of all authorized devices such as workstations, laptops, switches, routers, firewall, printers, scanner, photocopiers, etc. used to process, store or transmit data/information in the Agency/Organization

iii. Ensure the existence of an effective Risk Management Framework which serves to reduce the incidence of significant adverse impact on an organization by addressing threats, mitigating exposure, and reducing vulnerability.

iv. Incorporate cyber-risk management with their institution-wide risk management framework and governance requirements to ensure consistent management of risk across the organization/Agency/institution

v. Ensure the Board and Senior Management shall support and be involved in the cyber-risk management process by ensuring that resources and capabilities are available, and roles of staff properly defined in management of risks

vi. Ensure that risk assessments are updated regularly to address changes or introduction of new technologies, products etc. before deployment to ensure accurate risk measurement.

vii. Ensure risk treatment options such as risk reduction, risk retention, risk avoidance, risk transfer and how residual risk is addressed should be selected based on the outcome of the risk assessment.

viii. Ensure Information obtained from risk management activities shall be reported to the Senior Management and the Board of Directors to support informed decision making.

ix. Ensure applicable MDAs & ICT Private consistently conduct risk assessments, vulnerability assessments and threat analysis to detect and evaluate risk to their Information assets and determine the appropriateness of security controls in managing risk.

x. Implement a vulnerability management strategy; approved by the Director General/Board of Directors/MD/CEO/Senior Management/Chief Information Security Officer (CISO).

xi. Establish an automated mechanism to detect all vulnerabilities in its assets. This includes but is not limited to workstations, network devices, servers (production, test and development), etc. The vulnerabilities and threats shall be documented; potential business impact and likelihood shall also be identified.

xii. Conduct vulnerability assessment at least **quarterly** or whenever there is a significant change (such as installation of new systems, devices, applications, etc.) to the information processing infrastructure or when vulnerabilities are made known.

5 CYBERSECURITY AWARENESS CAMPAIGN, CAPACITY BUILDING

OBJECTIVE

The objective of this section is to establish and give guidance on the implementation of national cyber security awareness campaign and capacity building.

ROLES AND RESPONSIBILITIES OF MDAs and PRIVATE ICT ORGANIZATIONS

MDAs and PRIVATE ICT ORGANIZATIONS SHALL:

Ensure capacity building and awareness in relations to Cyber Security Knowledge with the employee

Ensure and develop capacity building awareness plan and material should have both NITDA and the organization/Agency's content

6 INTERNET SAFETY AND CHILD ONLINE PROTECTION

OBJECTIVE

The objective of this section is to establish and give guidance on the implementation of Internet safety and child online protection.

ROLES AND RESPONSIBILITY OF NITDA

NITDA SHALL:

i. Develop framework for assessing as is, scope, identification, reporting, prosecution and publicity.
ii. Work with service providers to shut offensive sites. Conduct constant monitoring.
iii. Improve national awareness on cybersecurity/internet safety across all segments of the Nigerian society through targeted awareness campaign/advocacy.
iv. To provide Nigerians with information to protect themselves, families and organizations online through raising awareness of the Cybercrime Act, 2015, trends of evolving cyber threats with mitigation measures.
v. Establish a Cybersecurity Centre of Excellence in one university in each geo-political zone in Nigeria.
vi. Create a roadmap for empowering cybersecurity professionals to develop local ICT content and innovation

Individual agencies should contribute to child online protection by

a) Educating parents on the need to limit access to obscene contents
b) Report incidences.

ROLES AND RESPONSIBILITY OF MDA'S/PRIVATE ICT ORGANIZATIONS

MDA'S/PRIVATE ICT ORGANIZATIONS SHALL:

i. Educate employees, contractors and customers on cybersecurity so as to mitigate cyber-attacks within the Agency/Organization using different delivery mediums such as, Instructor led training, classroom-based, E-learning, distance learning, web-based, TV, and Radio.
ii. Ensure Board members/Senior Management and employees participate during the training program.
iii. Ensure that an information/Cyber security awareness program is established in line with the organization's business objectives.

iv. Ensure information security policies and relevant procedures have taken into consideration the organization’s information to be protected and the controls that have been implemented to protect the information.

v. Always update the Information/ Cyber Security awareness program regularly to ensure compliance with organizational policies and procedures and should be built on lessons learnt from information security incidents.

vi. Awareness training should be performed as required by the organization’s information security awareness program. Awareness training can use different delivery media including instructor led training, classroom-based, E-learning, distance learning, web-based, self-paced and others.

vii. Develop school-based awareness program on cyber safety for primary and secondary schools.

viii. Establish a working mechanism for reporting illegal content of child sexual abuse found on the internet

ix. Build capacity and provide forensic tools for Law Enforcement Agencies (LEAs) to investigate internet related crimes against children and young people and maintain a register of such offenders.

x. Ensure R&D Endowment Interventions in selected Nigerian Universities to support setting up of Cybersecurity Centre of Excellence.

xi. Supports Indigenous ICT Institutes on software and hardware development

xii. Sponsor innovative research outputs in various aspects of Cyber security

xiii. Ensure Selected Centers of Excellence are involved in (Critical Infrastructure Program for Modeling and Analysis CIPMA program

xiv. Promote cybersecurity research, innovation & local content development.

7 PUBLIC PRIVATE PARTNERSHIP

OBJECTIVE

The objective of this section is to establish and give guidance on the Implementation of public and private partnership

ROLES AND RESPONSIBILITY OF NITDA

i. Develop public-private information sharing arrangements and protocol.

ii. Engage owners and operators of Nigeria's critical infrastructure, key network asset owners including the private sector on technological innovations, critical resources and technical standards required for their seamless operations.

iii. Build national capabilities against cyber threats through collaboration among public-private sector partners and multi-stakeholder engagement.

iv. Engage States and Local Governments on cybersecurity, seek their active involvement in securing computer systems and networks and other facilities within their jurisdiction.

v. Build a trusted platform for strategic information sharing between government and private sector to proactively identify, monitor and respond to cyber threats.

vi. Establish a Public-Private Partnership (PPP) National Technical Working Group (NTWG) on cybersecurity. Establish a public-private information sharing forum to help combat cyber-attack and create a cyber resilient culture within All MDAs & Private ICT Organizations.

vii. Create private sector and state government led PPP initiatives on improving cybersecurity at state and local government levels.

viii. Develop the objective to build national capabilities against cyber threats through collaboration among public-private sector partners and multi-stakeholder engagement

ix. Engage State and Local Governments on cybersecurity; seek their active involvement in securing computer systems and networks and other facilities within their jurisdiction.

x. Develop public-private information sharing arrangements and protocol with the objective to build a trusted platform for strategic information sharing between government and private sector to proactively identify, monitor and respond to cyber threats.

xi. Supports the PPP arrangement for Protection of Critical Information Infrastructure (CII), computer and network assets with impact on the economy and security.

xii. Engage operators of Nigeria's critical infrastructure and key stakeholder owners of network assets including the private sector on technological innovation, critical resources and technical standards required for their seamless operations.

xiii. Coordinates timely response to national/international cybersecurity challenges.

xiv. Ensure it is equipped with a minimum of one CSIRT team in each geopolitical zone.

xv. Ensure a designated functional platform for information sharing of the public and private sectors.

xvi. Ensure regular or periodic feedback from regulating agencies and access to information on threats and vulnerabilities of private sector.

xvii. Ensure it establishes the Critical Information Infrastructure Program modeling and Analysis Critical Infrastructure Program for Modeling and Analysis (CIPMA).

8 CYBERSECURITY OPERATIONAL RESILIENCE

OBJECTIVE

The objective of this section is to establish and give guidance on the Implementation of Cyber Security Operational Resilience.

ROLES AND RESPONSIBILITY OF MDA'S/PRIVATE ICT ORGANIZATIONS

MDAs and PRIVATE ICT ORGANIZATIONS SHALL:

Continuously improve on their cyber security resilience. This is crucial for the prompt identification of system vulnerabilities; emerging threats and their associated risks; rapid cyber-incident response; increasing cybersecurity maturity levels; ensuring the confidentiality, integrity and availability of information assets whilst promoting a safe and effective Cyber Resilient Posture within all MDAs and ICT Organizations in Nigeria.

9 METRICS, MONITORING & REPORTING

OBJECTIVE

The objective of this section is to establish and give guidance on the implementation of metrics, Monitoring & Reporting.

ROLES AND RESPONSIBILITY OF MDA'S/PRIVATE ICT ORGANIZATIONS

MDAs and PRIVATE ICT ORGANIZATIONS SHALL:

i. Put in place metrics and monitoring processes to ensure compliance, provide feedback on the effectiveness of control and the basis for appropriate management decisions. The metrics should properly align with strategic objectives and provide the information needed for effective decisions at the strategic, management and operational levels.

ii. Establish effective and reliable reporting and communication channels between NITDA and NGCERT.

iii. Establish a reporting process that defines reporting and communication channels for the dissemination of security-related material such as changes in policies, standards, procedures, new or emerging threats and vulnerabilities.

iv. Report all cyber-incidents whether successful or not within one hour of Identification to the management or Director General or the CEO/MD.

ROLES AND RESPONSIBILITY OF PRIVATE ICT ORGANIZATIONS THAT OFFER CYBER SECURITY SERVICES

Private ICT organizations that offer Cyber Security Services shall register with NITDA and periodically (quarterly) submit to NITDA a technical report of their activities, indicating

a) Overview of deployments of tools, devices, software, personnel etc

b) Allow NITDA access to assess their infrastructure to forestall possible unsavory conduct.

c) Service delivery to MDAs and other private companies should be over regulated by NITDA;

10 COMPLIANCE WITH STATUTORY AND REGULATORY REQUIREMENTS

OBJECTIVE

The objective of this section is to give guidance on the implementation of compliance with statutory and regulatory requirements.

To ensure the relevant stakeholders, government and private organizations comply with statutory and regulatory requirements defined in this and other related documents.

ROLES AND RESPONSIBILITIES OF NITDA

NITDA shall monitor and enforce compliance with the provisions of the Guidelines.

Effective Date : This Guideline shall take effect from Nov 1, 2019.

ROLES AND RESPONSIBILITY OF MDA’S/PRIVATE ICT ORGANIZATIONS

MDA’S/PRIVATE ICT ORGANIZATIONS SHALL:

Comply with all relevant statutes and regulations such as the Nigerian Cybercrimes (Prohibition, Prevention etc.) Act, 2015 and all NITDA, National Information Technology Agency directives to avoid breaches of legal, statutory, regulatory obligations, related to cyber security and of any security requirements.

APPENDIX I

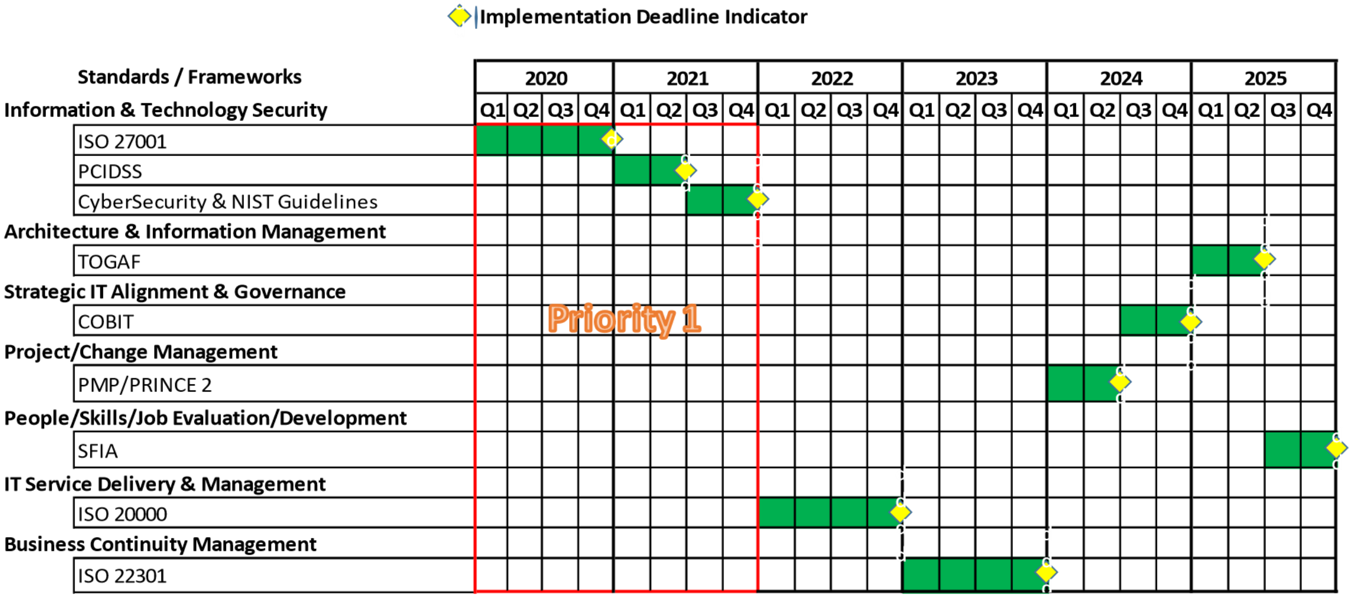
CISO: RELEVANT SKILLS & QUALIFICATIONS REQUIRED

- Develop, implement and monitor a strategic, comprehensive enterprise information security and IT risk management program
- Work directly with the team and units to facilitate risk assessment and risk management processes
- Develop and enhance an information security management framework
- Understand and interact with related disciplines through committees to ensure the consistent application of policies and standards across all technology projects, systems and services
- Provide leadership to the enterprise's information security organization/Agency
- Partner with stakeholders across the Agency/Organization to raise awareness of risk management concerns
- Assist with the overall technology planning, providing a current knowledge and future vision of technology and systems
- Excellent communication skills (oral, written, presentation and listening) with ability to influence and negotiate with people at all levels inside and outside the Agency/organization
- Degree in the Information Security field, business administration or equivalent qualification/experience
- Master's in cyber/Information Security
- A good understanding of IT technologies and architectures in relation to Information Security
- Professional security management certification e.g. CISSP, CISM
- Minimum of eight (8) to ten (10) years of experience in a combination of risk management, information security & IT jobs
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, ISO/IEC 22301 and NIST, PCI DSS
- Excellent written and verbal communication skills and high level of personal integrity
- Innovative thinking and leadership with an ability to lead and motivate cross-functional, interdisciplinary teams
- Experience with contract and vendor negotiations and management including managed services

PROPOSED STANDARDS & FRAMEWORKS IMPLEMENTATION ROADMAP

For MDAs

NITDA Cybersecurity IT Standards & Frameworks Implementation Roadmap



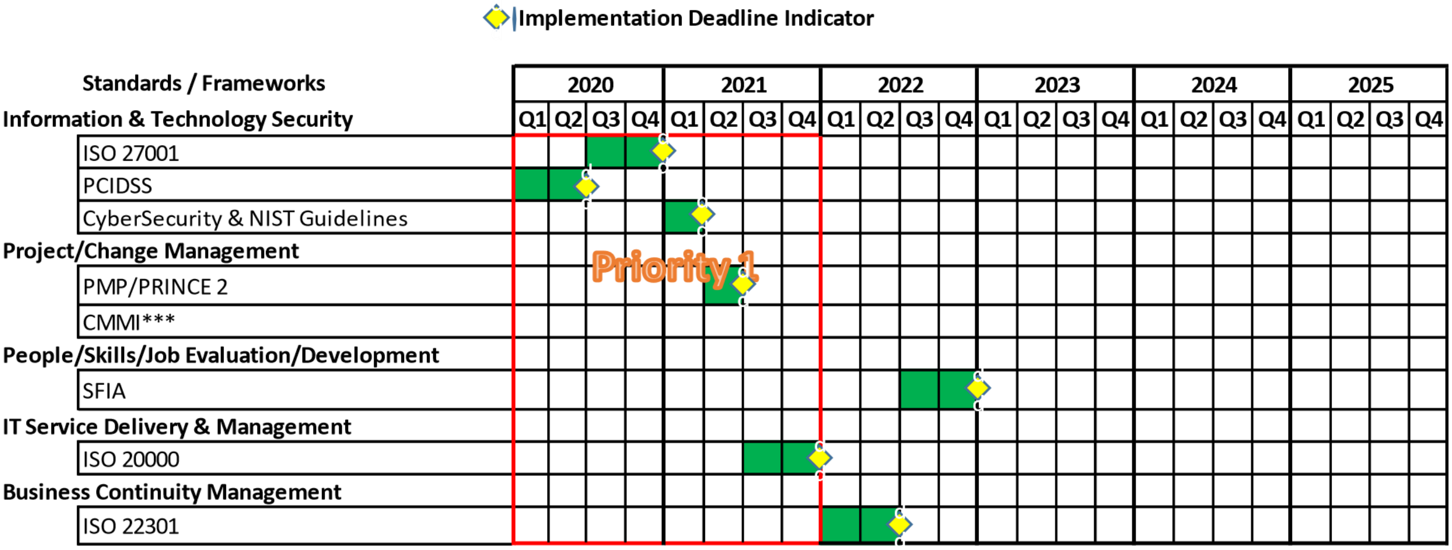
◆ Implementation Deadline Indicator

Standards / Frameworks	2020				2021				2022				2023				2024				2025			
Information & Technology Security	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ISO 27001	🟩	🟩	🟩	🟩◆																				
PCIDSS					🟩	🟩◆																		
CyberSecurity & NIST Guidelines							🟩	🟩◆																
Architecture & Information Management																								
TOGAF																					🟩	🟩◆		
Strategic IT Alignment & Governance																								
COBIT																			🟩	🟩◆				
Project/Change Management																								
PMP/PRINCE 2																	🟩	🟩◆						
People/Skills/Job Evaluation/Development																								
SFIA																							🟩	🟩◆
IT Service Delivery & Management																								
ISO 20000									🟩	🟩	🟩	🟩◆												
Business Continuity Management																								
ISO 22301													🟩	🟩	🟩	🟩◆								

COBIT: Minimum process capability levels of 2 required for top 15 processes derived from Goals Cascade Process

For Private and ICT Organizations

NITDA Cybersecurity IT Standards & Frameworks Implementation Roadmap



◆ Implementation Deadline Indicator

Standards / Frameworks	2020				2021				2022				2023				2024				2025			
Information & Technology Security	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4
ISO 27001			🟩	🟩◆																				
PCIDSS	🟩	🟩◆																						
CyberSecurity & NIST Guidelines					🟩◆																			
Project/Change Management																								
PMP/PRINCE 2						🟩◆																		
CMMI***																								
People/Skills/Job Evaluation/Development																								
SFIA											🟩	🟩◆												
IT Service Delivery & Management																								
ISO 20000							🟩	🟩◆																
Business Continuity Management																								
ISO 22301									🟩	🟩◆														

*** - only applicable to software development organizations. A minimum compliance level 3 is required.

APPENDIX II CYBER HYGIENE PRACTICES

This chapter covers the threat agents and vulnerabilities that expose citizens to online risks and preventative measures to reduce likelihood of falling victim of an attack, i.e "attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset" (ISO/IEC 27000: 2014)

We have adopted the European Union Agency For Network and Information Security , ENISA's top ten ***general*** practices to maintain cyber hygiene[1] are as follows:

1. Have a record of all hardware so you know what your estate looks like
2. Have a record of all software to ensure it is properly patched
3. Utilise secure configuration / hardening guides for all devices
4. Manage data in and out of your network
5. Scan all incoming emails
6. Minimise administrative accounts
7. Regularly back up data and test it can be restored
8. Establish an incident response plan
9. Enforce similar levels of security across the supply chain
10. Ensure suitable security controls in any service agreements (including cloud services)

Controls to strengthen specific domains in the sections that follow are adapted from ISO 27032.

3.1 End-user controls

The following is an incomplete list of controls that end-users can use to protect their systems against known exploits and attacks:

1. **Use of supported operating systems, with the most updated security patches installed.** Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding supported operating systems. Individual consumers should be aware of, and consider using, provider recommended operating systems. In all cases, the operating system should be kept up to date regarding security patches**. Illegally obtained licenses are forbidden**.
2. **Use of the latest supported software applications, with the most updated patches installed.** Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding supported application software. Individual consumers should be aware of, and consider

[1] ENISA

using, provider recommended application software. In all cases, the application software should be kept up to date regarding security patches.

3. **Use anti-virus and anti-spyware tools.** If feasible, a service provider such as an ISP should consider partnering with trusted security vendors to offer end-users these tools as part of the service subscription package so that the security controls are made available upon signing-up the subscription, or upon renewal. Organizational consumers have a responsibility to be aware of, and follow, organizational policy regarding the use of security software tools. Individual consumers should use security software tools. They should look to the provider for any recommended, provided, or discontinued security software. In all cases, the security software should be kept up to date regarding security patches and signature databases.
4. **Implement appropriate anti-virus and anti-spyware safeguards**. Common web browser and browser toolbars have now incorporated capabilities such as pop-up blockers, which will prevent malicious websites from displaying windows that contain spyware or deceptive software that could exploit system or browser weaknesses, or use social engineering to trick users into downloading and installing them on their systems. Organizations should establish a policy to enable the use of such tools. Service providing organizations should collate a list of recommended tools, and their use should be encouraged to end-users, with guidance on their enablement and permission granting for websites that users would like to allow.
5. **Enable script blockers**. Enable script blockers or a higher web security setting to ensure that only scripts from trusted sources are executed on a local computer.
6. **Use phishing filters**. Common web browser and browser toolbars often incorporates this capability, which could determine whether a site that a user is visiting is found within a database of known phishing websites, or contains script patterns that are similar to those found typical phishing websites. The browser would provide alerts, normally in the form of colour-coded highlights, to warn users of the potential risk. Organizations should establish a policy to enable the use of such tool.
7. **Use other available web browser security features**. From time to time, as new Cybersecurity risk emerges, web browsers and browser toolbar providers add new security capabilities to protect users against risks. End-users should keep abreast of these developments by learning about such updates that are normally provided by the tool providers. Organizations and service providers should similarly review these new capabilities and update related policies and services to better serve the needs of their organizations and customers, and address related Cybersecurity risk.
8. **Enable a personal firewall and Host based Intrusion Detection System, HIDS.** Personal firewalls and HIDS are important tools for controlling network services accessing the user systems. A number of newer operating systems have personal firewalls and HIDS incorporated. While they are enabled by default, users or applications might disable them, resulting in undesirable network security

exposures. Organizations should adopt a policy on the use of a personal firewall and HIDS and evaluate suitable tools or products for implementation so that their use is enabled by default for all employees. Service providers should encourage the use of a personal firewall and HIDS functions, and/or suggest other third-party personal firewall and HIDS products that has been evaluated and considered as trusted, and educate and help users in enabling basic network security at the end-user system level.

9. **Enable automated updates**. While the above technical security controls are capable of dealing with most malicious software at their respective operating levels, they are not very effective against exploitation of vulnerabilities that exist in operating systems and application products. To prevent such exploits, the updating function available in operating systems, as well as those provided by user-trusted applications (for example, trusted third-party evaluated anti-spyware and anti-virus products), should be enabled for automated updates to be performed. This would then ensure that systems are updated with the latest security patches whenever they are available, closing the time gap for exploits to take place.

3.2 Server protection

The following controls can be used to protect servers against unauthorized access and the hosting of malicious content on servers:

1. **Server Configuration**: Configure servers, including underlying operating systems in accordance to a baseline security configuration guide as provided in the implementation toolkit. This guide includes proper definition of server users versus administrators, enforcement of access controls on program and system directories and files, and enabling of audit trails, in particular, for security and other failure events on the system.
2. **Server Usage:** It is recommended to install a minimal system on a server in order to reduce the attack vector.
3. **Security Updates**: Implement a system to test and deploy security updates, and ensure the server operating system and applications are kept up-to-date promptly when new security updates are available.
4. **Server Monitoring**: Monitor the security performance of the server through regular reviews of the audit trails.
5. **Configuration Review:** Review the security configuration every 3 months.
6. **Anti-malware**: Run anti-malicious software controls (such as anti-virus and anti-spyware) on the server. Scan all hosted and uploaded content regularly using up to date anti-malicious software controls.

7. **Vulnerability Assessment and Penetration Testing:** Perform regular vulnerability assessments and security testing for the online sites and applications to ensure that their security is adequately maintained; and regularly scan for compromises.

3.3 Application level controls

1. **Web Application Handling**: Ensure secure handling of sessions for web applications including mechanisms such as cookies.
2. **Secure Input Validation:** Ensure secure input validation and handling to prevent common attacks such as SQL-Injection. Based on the fact that websites, which are generally considered as trustworthy, are increasingly used for malicious code distribution, input and output validation have to be carried out by active content as well as by dynamic content.
3. **Cross-Site Scripting Controls:** Secure web page scripting to prevent common attacks such as Cross-site Scripting.
4. **Code Review**: Ensure Code security review and testing by appropriately skilled entities.
5. **Web Service Authentication:** the organization shall use HTTPS credentials registered to it.

3.4 Controls against social engineering attacks

The Do's:

- Understand personal responsibility with regard to information security and maintain knowledge of corporate policies on software usage, network/Internet usage of antivirus software, and anti-spyware usage.
- Question strangers in your premises who are not properly identified
- Wear your identity card in such a way that is visible to other people
- Keep informed about the established security rules, apply them and, if unclear, seek guidance.
- Be aware of the types of security incidents that can and do occur.
- Report security incidents and concerns about:
- Poorly controlled or error-prone electronic transactions
- Equipment issues, such as unknown origin, broken equipment, etc.
- Access violations
- Inadequate backups
- System unavailability
- Make regular backups of critical data and periodically test the backups to ensure that data can be restored
- Change passwords immediately upon receipt and then regularly in accordance with policy.

- Ensure that the chosen password is difficult to guess and meets established best practices for length, complexity, unacceptable names, etc.
- Lock rooms and check the desktop when leaving important data or equipment behind.
- Remember that anything written in an e-mail may be held against the writer or his/her enterprise and that this evidence can be kept forever
- Dispose of sensitive information effectively—shred, wipe disks, destroy media, etc.
- Return all company materials, including data files, upon termination of employment
- Beware of free USB’s given as gifts at seminars as it may contain a malware which could create a backdoor to your processing assets. Always format your removable USB device for the first time.
- Ensure removable storage devices are encrypted in transit and at rest
- Should sensitive authentication credentials get lost through the loss of flash drives, change the passwords, PINs, security questions and answers immediately. If necessary, report loss to incident response team
- Switch off wired/wireless routers when not in use.
- Always turn off Bluetooth and wiFi network after use.
- Update mobile operating system regularly
- Follow a regular backup procedures for your mobile devices
- Ensure your device is password-protected
- Only install mobile apps verified by App Store or Play Store

The Don’ts:

- Don’t Use enterprise computing resources for unapproved purposes (e.g., intellectual property protection violations, illegal content)
- Don't leave the system unattended and accessible for extended periods of time
- Don’t tell anyone your password or share any other authentication token with anyone (except properly authorised group passwords)
- Don’t disclose sensitive data to anyone who is not authorised to receive them or who does not need to know them
- Don’t load or use pirated software or unqualified shareware onto any enterprise computer
- Don’t bypass established network connection rules
- Do not store sensitive data on flash drives without strong encryption or password
- USB devices such as cell phones, Mp3 players, digital cameras, etc, should be properly scanned for malware.
- Avoid connecting your phone to an unknown external port to charge.

- Avoid clicking links from unverified sources in your email.
- Don’t leave devices unattended and out of sight in public places such as at airports, in taxis, at restaurants, inside car, etc
- Avoid connecting to unknown networks, especially “free wiFi”
- Only install mobile apps verified by App Store or Play Store