UGANDA COMMUNICATIONS COMMISSION

THE UGANDA COMMUNICATIONS COMMISSION

MINIMUM CYBERSECURITY GUIDELINES FOR THE LICENSED OPERATORS IN UGANDA

JUNE 2025

Board Chairperson: *Signature* _____ *Date* 30.06.2025

Executive Director: *Signature* _____ *Date* 14/8/25

TABLE OF CONTENTS

TABLE OF CONTENTS 2
1 DEFINITIONS 3
2 INTRODUCTION 5
3 APPLICATION 6
4 PURPOSE 6
5 APPLICABLE LEGISLATION AND REGULATIONS 6
6 GENERAL PROVISIONS 7
6.1 RISK-BASED APPROACH 7
6.2 RELEVANT STANDARDS 7
6.3 CYBERSECURITY GOVERNANCE AND MANAGEMENT CONTROLS 7
6.3.1 Cybersecurity Oversight and Governance 7
6.3.2 Cyber Security Risk Management 9
6.3.3 Cybersecurity Assessment and Auditing 9
6.4 Incident and Disaster Recovery Management 10
7 ENFORCEMENT AND REMEDIAL MEASURES 10
8 PART 1: INTERNET SERVICE PROVIDERS (ISPs) 11
8.1 Cyber Security Technical and Operational Controls 11
9 AMENDMENT 13
10 ANNEX 1: LIST OF STANDARDS 13

1 DEFINITIONS

The terms in these Guidelines shall carry the interpretation used in the Uganda Communications Act 2013 (The Act) and respective Regulations thereto, unless otherwise defined below:

Term	Definition
Audit	Independent review of records and activities to assess system controls adequacy and ensure compliance with established policies and operational procedures
Authentication	Verifying a user, process, or device is often a prerequisite to allowing access to resources in an information system. Or provision of assurance that a claimed characteristic such as identity, role, or permissions of an entity is correct
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges
Availability	Ensuring timely and reliable access to and use of information Or the property of being accessible and usable on demand by an authorized entity
Critical Communication Information Infrastructure (CCII)	CCII refers to the essential communication systems and networks that underpin the functioning of other critical sectors in Uganda
Criticality	A measure of the degree to which an organization depends on the information or information system for the success of a mission or a business function including both critical infrastructure and essential business processes.
Cyber Resiliency	The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation
Cyber Threat	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Disaster	An incident, either man-made or natural, sudden, or progressive, the impact of which is such that the affected organization must respond through exceptional measures

	such as activating a disaster recovery plan or invoking a business continuity procedure to manage and mitigate the effects/impact
Event	Any observable occurrence in a network or information technology, service, or system
Governance	A set of processes that ensures that assets are formally managed throughout the enterprise
Guideline	A set of recommendations or goals that can be used when there are no specific standards/procedures in place, or they do not apply
Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies
Information Asset	Any resource that the licensee possesses or employs to support information-related activities
Licensed Operators	A licensed operator is any entity that has been licensed by UCC to provide services in the communications sector. This includes telecommunication companies, Internet Service providers, broadcasters like TV and radio stations, satellite providers and courier companies
Operator	Operator means a person licensed to provide a communication or broadcasting service. "person" includes any individual, company, association, or body of persons corporate or unincorporated
Policy	Set of formal statements, rules, or guidelines that define the acceptable and expected behaviors, procedures, and decisions within an organization, covering areas like security, operations, and business conduct
Procedure	Set of activities or steps taken to achieve business process goals or apply policy
Security Standard	A set of published specifications that are designed to enhance the organizational, sectoral, national, and international security posture
Sensitivity	A measure of the degree to which an IT (Information Technology) system or application requires protection (to ensure confidentiality, integrity, and availability) which is determined by an evaluation of the nature and criticality of the data processed, the relation of the system to the organization missions and the economic value of the system components
Strategy	A high-level and long-term plan of action designed to achieve the desired objectives
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

2 INTRODUCTION

The Uganda Communications Commission (UCC) acknowledges the dynamic nature of cyberspace and the crucial necessity for robust cybersecurity measures to safeguard the nation's digital infrastructure. In response, UCC has formulated the Minimum Cybersecurity Guidelines for licensed operators in Uganda. These guidelines, meticulously designed, serve to fortify the security landscape in the digital realm, bolstering the security posture of licensed operators and ensuring dependable services for Ugandan citizens.

Aligned with the Uganda Communications (Computer Emergency Response Team) Regulations of 2019, specifically sections 9(a) and (d), which stipulate secure transmission environments and adherence to CERT guidelines, these directives have the potential to continually enhance cybersecurity preparedness, cultivate customer trust, and diminish the impact of cyber incidents.

The Commission recognizes the pivotal role of the Internet in propelling economic growth, ameliorating access to services and information, and nurturing education, healthcare, innovation, and entrepreneurship in Uganda. It remains a paramount driver of progress in the nation.

The ICT sector, central to Uganda's socioeconomic transformation as per the National Vision 2040, underpins the national economy's competitiveness through broadband, online services, and information assets. Given the escalating demands for service availability, user experience, and data protection, reinforcing cybersecurity becomes paramount to bolstering trust in Uganda's resilient ICT infrastructure.

Cyberspace stands as a battleground between cybercriminals and law enforcement. The fourth National Development Plan (**NDPIV**) 2025/26 - 2029/30 underscores Uganda's imperative to bolster communication structures, anticipating and mitigating disruptions and misinformation. UCC is committed to regulating cyberspace, enhancing resources for cyber defense, and safeguarding critical infrastructure.

ICT in Uganda functions as critical infrastructure, forming the bedrock of various sectors. Hence, securing ICT infrastructure is vital to ensure connectivity, data confidentiality, service continuity, and national security. Licensed operators must prioritize cybersecurity by implementing these guidelines alongside advanced frameworks, standards, and practices.

The rapid technological advancement offers immense opportunities, enhancing efficiency and accuracy. However, it also introduces new risks. Addressing these risks is paramount for a secure digital environment, aligning with the Communication Sector Cybersecurity Strategy (2022-2027) and the Computer Emergency Response Team Regulations of 2019.

These guidelines transcend compliance by emphasizing the allocation of cybersecurity capabilities across people, technologies, and processes. While outlining mandated requirements, they offer licensed operators the flexibility to implement additional security controls tailored to their activities. Determining security levels entails considering risk appetite, business needs, and the value of information assets.

3 APPLICATION

The guidelines outlined here shall apply to all licensed operators in Uganda. Nevertheless, distinct guidelines will be formulated for the various subsectors within the Communication sector. These subsectors encompass Internet Service Providers, Broadcasting, Radio Communications, Postal Communications, and more. These specific guidelines will be crafted to guarantee thorough coverage and relevance tailored to each corresponding subsector.

4 PURPOSE

These guidelines define the minimum, common, and harmonized cybersecurity controls that will be implemented by licensed operators to protect critical Communication Information Infrastructure.

5 APPLICABLE LEGISLATION AND REGULATIONS

The following documents, statutory instruments, regulatory and operational frameworks shall apply to the implementation of these guidelines:

a) Uganda Communications Commission Act, 2013.
Section 5(1) of the Uganda Communications Act of 2013, which spells out the functions of the Commission as including.
   I) *implement the objectives of the Act.*
   II) *monitor, inspect, license, supervise, control, and regulate communications services.*
   III) *promote and safeguard the interests of consumers and Operators as regards the quality of Communications services and equipment.*
b) Data Protection and Privacy Act, 2019.
c) Computer Misuse Act, 2011.
d) The National Payments Systems Act 2020
e) The Electronic Transactions Act, 2011
f) The Electronic Signature Act 2011
g) Uganda Communications (Computer Emergency Response Team) Regulations, 2019
h) The Uganda Communications(Equipment Type approval) Regulations 2019.
i) The Telecommunications (Consumer Protection) Regulations, 2019
j) Communications Sector Cyber Security strategy, 2022-2027
k) Operator license agreements issued by the Commission.

6 GENERAL PROVISIONS

6.1 RISK-BASED APPROACH

Recognizing the dynamic nature of cyber threats and the varying risk profiles of licensed operators, these guidelines emphasize the importance of adopting a risk-based approach and conducting comprehensive risk assessments.

a) licensed operators shall identify and evaluate potential threats and vulnerabilities specific to their operations. This allows them to prioritize their cybersecurity efforts and allocate resources effectively to address the most significant risks.

b) licensed operators shall proactively identify and mitigate cybersecurity risks, safeguard their systems and networks, and ensure the continuous provision of secure internet services to users across Uganda.

6.2 RELEVANT STANDARDS

The guidelines have been developed considering relevant UCC regulations, frameworks, and international best practices and standards. The Commission recognizes various international, regional, and national standards concerning information security and cyber security management. Annex 1 contains a list of such standards.

In adopting international standards, the Commission may:

I. Adopt the standard as is.
II. Make editorial changes without altering the technical content of the standard.
III. Make changes in the technical content to address national requirements.

6.3 CYBERSECURITY GOVERNANCE AND MANAGEMENT CONTROLS

Under section 9 of the CERT Regulations of 2019, by implementing Cybersecurity Governance and Management practices, licensed operators shall ensure that cybersecurity is treated as a strategic priority to enable effective decision-making, risk management, and operational implementation of cybersecurity measures.

6.3.1 Cybersecurity Oversight and Governance

a) Licensed operators shall establish, adopt, and ingrain a cybersecurity governance framework for implementing and managing the cybersecurity program with clear roles and responsibilities.
b) The Board of Directors or equivalent shall be responsible and accountable for cybersecurity management for the licensed operator

and shall be responsible for but not limited to.

i. Approving and overseeing the cybersecurity program, strategy, and policy to manage cyber risks as well as supporting the culture of awareness of cybersecurity in the organization and the customers. The above-mentioned documents shall be shared with the Commission.
ii. Being supportive and engaged in cyber risk resiliency and posture assessments, communication sector evolving trends of cyber risks, threats, and any cybersecurity-related initiatives.
iii. Allocating adequate budget and resources for fulfilling cybersecurity requirements.
iv. Investing in cybersecurity capabilities and allocating resources to implement and maintain effective security controls in line with organization strategy.
v. Periodically review and update licensed operators' cybersecurity strategy, program, and policy to address emerging threats and evolving technologies.

c) The board of directors or equivalent shall delegate cybersecurity-related responsibilities to a dedicated cybersecurity steering committee that is established and mandated by the board.
d) Establish an independent cybersecurity steering committee or incorporate cybersecurity committee mandates within an existing committee. This is to ensure leadership support in the implementation of cybersecurity requirements across the organization.
e) The licensed operators shall institutionalize the cybersecurity function to ensure an appropriate level of independence of any other role that might conflict with the cybersecurity program and objectives, including reporting path, budget, and resources. Operators shall have a cybersecurity representative at the senior management level. The representative would act as a key liaison, effectively articulating the evolving cyber landscape, potential risks, and mitigation strategies to ensure informed decision-making at the highest level.
f) The licensed operators shall establish, implement and maintain an appropriate process for managing changes in personnel (employees, contractors, third-party users) or changes in their roles and responsibilities. New personnel should be briefed and educated on the policies and procedures in place. Accounts, rights, possession of equipment, or data should be reviewed regarding personnel changes.
g) The licensed operators shall define a cybersecurity strategy and develop an implementation roadmap to achieve the defined objectives of the strategy. The defined road map shall be shared with the Commission.
h) The licensed operator shall establish, implement and maintain an appropriate information security/cybersecurity policy. The policy shall be shared with the Commission.
i) The licensed operator shall establish, implement, and maintain an appropriate information security/cybersecurity policy, which shall be submitted to the Commission.

j) Licensed operators shall provide their customers with relevant cybersecurity information related to the provided service to improve cybersecurity awareness.
k) Licensed operators shall adopt a comprehensive and continuous cyber security approach that encompasses threat prediction, prevention, detection, response, and investigation.
l) In collaboration with key stakeholders, Licensed operators shall develop, implement, and support cybersecurity public awareness campaigns targeting consumers, children, and people with special needs.

6.3.2 Cyber Security Risk Management

A licensed Operator shall:

a) Establish, enforce, and maintain a systematic approved cyber risk management process/approach aligned with the enterprise risk management process to protect the Confidentiality, Integrity, and Availability (CIA) of identified information and technological assets.
b) Perform Cybersecurity risk assessment for targeted environments such as critical business environments, business processes, and business applications including those under development regularly.
c) Establish and implement an appropriate cybersecurity risk treatment and monitoring approach to manage the identified risks and monitor the treatment plans.
d) Establish a corporate-wide supply chain management system based on third-party risk management (TRM) covering risk assessment, supplier relationship management, vulnerability management, and quality of products.
e) Ensure that compliance with the cyber security controls is subject to periodic review and audit.
f) Implement security by design, in ICT products and services that directly impact peoples' lives to ensure their safety.

6.3.3 Cybersecurity Assessment and Auditing

The assessment and auditing shall include network and information systems, facilities, and security measures/controls, including penetration testing. This comprehensive approach aims to ascertain with reasonable confidence:

- Whether cybersecurity controls have been designed and implemented securely.
- Whether the monitoring of these controls' effectiveness is being conducted consistently.
- Whether any vulnerabilities or weaknesses exist in the network, information systems, facilities, or security measures.

a) A licensed Operator shall establish and maintain an appropriate policy and processes for performing security assessments and security testing of all assets. [ISO27002: Chapter 15.2]
b) A licensed Operator shall establish and maintain policies for testing and exercising backup and contingency plans, where appropriate in collaboration with relevant third parties. [BS25999:Chapter8.3]
c) Licensed Operator shall conduct comprehensive annual cybersecurity assessments and audits, both internal and external, covering people, processes, and technology. These assessments shall include but not limited to penetration testing, vulnerability assessments, risk assessments, security audits, and social engineering testing.

6.4 Incident and Disaster Recovery Management

This section ensures operational continuity and data integrity for an operator in the face of unexpected disruptions. This involves meticulous planning, preparation, and execution to effectively respond to various incidents, ranging from cyberattacks, system failures, and natural disasters. The primary goal is to minimize the impact of such events on business operations, customer trust, and overall reputation.

Sections 9 (a), (e), and (f) of the Uganda Communications (Computer Emergency Response Team) Regulations 2019 require operators:

a) To notify the Commission of any significant information or computer security threat or incident that comes to their attention during the ordinary course of the business. In this context, "significant" refers to incidents or threats that have a notable impact on the organization's operations, data security, or reputation.
b) Provide the Commission with quarterly cyber security incident reports, information technology and risk assessment reports, and any other information requested by the Commission, therefore.
c) Allow inspectors access to records and premises during an investigation of any communications emergency or incident of alleged cybercrime.

7 ENFORCEMENT AND REMEDIAL MEASURES

Where the Licensed Operator fails to comply with any of the provisions or conditions of these guidelines, including failing to submit necessary information as mandated, such an operator shall be deemed guilty of contravening the provisions of the CERT Regulations. The applicable sanctions provided for by the CERT Regulations will be imposed.

8 PART 1: INTERNET SERVICE PROVIDERS (ISPs)

8.1 Cyber Security Technical and Operational Controls

Under Section (9) of the CERT Regulations of 2019, licensed ISPs shall:

a) Define, approve, communicate, implement, enforce, and monitor processes and procedures to manage the protection of business assets.
b) Define and implement a process to identify, assess, manage, and minimize the security risks of supply chains, contractors, vendors, suppliers, outsourcing, and third-party service providers.
c) Apply technical and operational security controls appropriate to the protected system's value, sensitivity, and criticality.
d) Establish change management procedures to minimize the likelihood of disruptions and errors due to changes. [ISO27011 Ch 10.1.2]
e) Define, approve, implement, and monitor the cybersecurity architecture, which outlines the cyber security requirements in the enterprise architecture and addresses the design principles for developing cyber security capabilities.
f) Define, approve, and implement the secure disposal standard and procedure for the information and technological assets. Businesses, customers, and other sensitive information must be protected from leakage or unauthorized disclosure when disposed of.
g) Implement real-time transaction monitoring and alerting systems to promptly detect and prevent fraudulent activities, anomalies, or potential security breaches.
h) Define and maintain a secure development lifecycle management process to ensure that security requirements are addressed during all phases of the software development lifecycle or acquiring new software.
i) Identify malicious traffic targeting systems and implement technical measures to filter and mitigate such traffic.
j) Establish and maintain threat intelligence processes to ensure the understanding of emerging and targeted cyber threats.
k) Where an ISP provides Digital Financial Services (DFS), such an ISP shall adopt a Digital Financial Services (DFS) security assurance framework. [ITU DFS SAF]
l) In Collaboration with the Commission, the ISP shall carry out periodic security tests of their DFS ecosystem.
m) Ensure that DFS applications are designed and implemented following industry and Standards Setting Bodies (SSB) best practices for secure software development.
n) Develop, adopt, and maintain a log retention policy and processes in line with the existing legal and regulatory frameworks. The information and records shall be maintained as per Regulation 10 (b) and (c) of the Uganda Communications (Computer Emergency Response Team) Regulations 2019.
o) Establish secure configuration standards for network devices, servers, and software applications, and regularly update and patch them to address known vulnerabilities and mitigate risks.

The licensed ISPs shall:

a) Define, approve, and implement cyber security incident management that is aligned with the enterprise incident management process, to identify, respond to, and recover from cyber security incidents. The effectiveness of this process should be measured and periodically evaluated. The approved cyber security incident management document shall be shared with the Commission. Cybersecurity Incidents shall be thoroughly investigated regardless. [ITU-T Rec. X.1056: Chapter 6.1]

b) Have the capacity to deal with security incidents, both internal and external to the internet service provider. The ISP shall have a team of individuals capable of handling security incidents as they occur. This team shall be a highly distributed functional team or a centralized security incident response team (e.g. security operations center).

c) Establish, adopt, and maintain appropriate procedures for reporting and communicating cybersecurity incidents as provided for in the Uganda Communications (Computer Emergency Response Team) Regulations 2019.

d) Report to the Uganda Computer Emergency Response Team (UG-CERT) under UCC all cybersecurity-related Incidents detected. The incidents shall include but not be limited to: -
    i. Intrusions to the ISP's network including intrusions to network infrastructure through SS7 exploits and fake base station attacks.
    ii. Breach of customer's data.
    iii. Denial of Service and Distributed Denial of Service Attacks.
    iv. Malware outbreaks.
    v. Spam-related incidents.
    vi. APT attacks such as Phishing attacks.
    vii. Spoofing-related attacks.
    viii. Web defacement.

e) Where the incidents impact the privacy and security of the customers, the ISPs shall inform the customer about the incidents, measures taken to handle the incidents, and measures the customers need to take to protect themselves.

f) Establish, implement, and maintain an incident response plan and procedures for handling security incidents. This includes: [ISO/IEC 27002: Chapter13.1]
    i. defining roles and responsibilities,
    ii. establishing communication channels including escalation procedures
    iii. conducting regular incident response cyber drills to ensure readiness and effective response.

g) The incident response plan shall, among other things, cover incident reporting, escalation procedures, response, and communication with

customers.

h) Establish and maintain an incident detection capability that detects cybersecurity incidents [ISO/IEC 27001: Chapter 4.2.3]

i) Implement a comprehensive logging and monitoring system to detect and respond to security incidents promptly. Monitor network traffic, system logs, and user activities to identify and mitigate potential threats.

j) Establish, implement, and maintain a comprehensive business continuity plan to ensure the continuity of reliable and dependable services to the customers. [ISO/IEC 27002: chapter14.1.3]

k) Establish, adopt, and maintain a Disaster recovery plan for critical ICT systems and be documented, tested, and maintained to support the business continuity plans. An appropriate disaster recovery capability shall be established to restore network and communication services after disasters. [ISO/IEC 27011: Chapter 14.1.3]

For additional guidance regarding the implementation, upkeep, and testing of disaster recovery plans, we suggest referring to the ISO 27031 guidelines, which provide insights into information and communication technology readiness for business continuity.

9 AMENDMENT

These guidelines will be regularly reviewed to maintain their relevance and may be updated to reflect new developments in the communications industry, changes in policies and regulations, and emerging international best practices.

10 ANNEX 1: LIST OF STANDARDS

ISO/IEC 27001:2013:	This International Standard specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system within the context of the organization. https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en
ISO/IEC 27002:2013:	This International Standard specifies a Code of practice for information security controls. https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en
ISO/IEC 27005:2018	This International Standard provides guidelines for

	information security risk management. https://www.iso.org/standard/75281.html
ISO/IEC 27011:2016	This international standard provides guidelines supporting the implementation of information security controls in telecommunications organizations. https://www.iso.org/standard/64143.html
ITU-T X.1051 :	Information security, cybersecurity, and privacy protection - Information security controls based on ISO/IEC 27002 for telecommunications organizations.
ISO/IEC 27031:2011	This international standard provides guidelines on information and communication technology readiness for business continuity: ISO/IEC 27031:2011 - Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity
ITU-T Rec.X.1056: Chapter 6.1	Security Incident Management guidelines for Telecommunications organizations.
SANS v6.1	SANS Institute Policy on Incident Handling.
ITU DFS SAF	The DFS Security Assurance Framework provides a systematic security risk management process for assessing threats and vulnerabilities and identifies appropriate security control measures to be implemented by the DFS provider and mobile network operator for threats targeting the user, mobile device, mobile network operator and DFS provider: https://www.itu.int/en/ITU-T/extcoop/figisymposium/Documents/ITU_SIT_WG_Technical%20report%20on%20Digital%20Financial%20Services%20Security%20Assurance%20Framework_f.pdf