



**NATIONAL COMPUTER AND CYBERCRIMES COORDINATION COMMITTEE
(NC4)**

**CYBERSECURITY STANDARDS FOR ADOPTION BY PUBLIC AND PRIVATE
ENTITIES GAZETTED AS CRITICAL INFORMATION INFRASTRUCTURE**

May 2025

1.0 Introduction

It is notable that there has been rapid spread, adoption and reliance on Information and Communication Technologies (ICTs) which has transformed service provision in Kenya. These ICTs have enhanced strategic and operational performance both in public and private sectors. However, the continual use of and digitization through ICTs has introduced threats and risks to these Critical Information Infrastructures.

ICT has been recognized as a strategic enabler, crucial to delivering the government's Bottom-Up Economic Transformational Agenda (BETA) and therefore, to capitalize on the opportunities presented by ICTs, cybersecurity standards of performance recommended for adoption by CIIs, MCDAs and Organizations this document outlines national and international standards/frameworks to secure our national ICT infrastructure.

The Government of Kenya has taken measures to manage and mitigate these threats through various initiatives such as enactment of the Computer Misuse and Cybercrimes Act 2018 (CMCA), Data Protection Act 2019 (DPA) and National ICT policy guidelines 2020; establishment of NC4, Gazettement of CIIs and adoption and implementation of information security management systems across government. These initiatives provide for adaptive response to cybersecurity threats based on regular risk assessments.

In regard to the above, Cyber security as a global phenomenon has embraced Management System Standards, frameworks and other best global practices in order to leverage and baseline with the researched and tested approaches towards more efficiency and management. This is envisaged to greatly improve the National Security posture with deep focus on the qualitative management of the national cyberspace.

2.0 Standard of performance to be adopted by CIIs

This document provides national and international standards to be adopted by CIIs, MCDAs and Organizations as mandated by CMCA SECTION 6(h) and CMCA regulations 60. Therefore, NC4 has published these standards. These include ICTA, ISO, GSMA and NIST.

International and National Information Security standards for adoption by Critical Information Infrastructure, MCDAs and Organizations

Vulnerability Management Standards	Cybersecurity and Privacy Protection Standards	Access Control Management Standards	Incident Management Standards
ISO/IEC 29147:2018	ISO/IEC 27555:2021	ISO/IEC 15816:2002	ISO/IEC 27035-3:2020
ISO/IEC 30111:2019	ISO/IEC 27018:2019		ISO/IEC 27035-2:2023
	ISO/IEC 27019:2024		ISO/IEC 27035-1:2023
	ISO/IEC 27006 1:2024		
	ISO/IEC TS 27006-2:2021		

Supply Chain Management Standards

ISO/IEC 28000:2022
ISO/IEC 27002:2022

Risk Management Standards

ISO 31000:2018
ISO/IEC 27005:2022

Information Security Management Standards

ISO/IEC 27001:2022
ISO/IEC 27002:2022
ISO/IEC 27007:2020

Cloud Security Management Standards

ISO/IEC 27017:2015
ISO/IEC 27018:2019
ISO/IEC 19086-4:2019
NIST SP 800-144

Network Security Standards

ISO/IEC 27033 Network Security series
GSMA NESAS
NIST SP 800 -41
IEC 62443

Application Security Standards

ISO/IEC 27002:2022
ISO/IEC 27034 Application Security series

National Information Security Standards

Information communication authority, government enterprise architecture framework provides minimum ICT plan and standards as guidelines on how to implement in government. Below are the ICTA

ICT Human Capital and Workforce Development - ICTA. 7.003: 2023

Government ICT Networks - ICTA.2.1.003:2023

Information Security Standard - ICTA-3.003:2023

Systems & Applications Standard - ICTA.6.003:2023

Electronic Records Management System Standard - ICTA.4.2.003:2023

Digitization of Public Records Standard - ICTA-4.3.003:2023

Fiber Optic-Backbone, Metro and Last Mile Infrastructure Standard First Edition 2021 - ICTA. 2.001:2021

Cloud Computing Standard -ICTA-8.003:2023

Data Centre Standard - ICTA.2.2.002:2023

End User Computing Standard - ICTA-2.3.002: 2023

Electronic Records Management Standard - ICTA-4.1.003:2023

ICT Governance Standard - ICTA. 5.003.2023

3.0 Conclusion

The adoption and compliance is critical to safeguard organization as well as provide confidence to the public and consumers that the various entities levels of compliance are in line with well recognized cybersecurity standards. Therefore, the Heads and Chief Executive Officers of the various CIIs must begin the process of adopting appropriate standards as well as build the necessary human resource critical mass and technical capabilities that will ensure Systems resilience to support their business operations and service to the people of Kenya.