

THE UNITED REPUBLIC OF TANZANIA

Supplement No. 24

19th June, 2026

SUBSIDIARY LEGISLATION

To The Gazette of the United Republic of Tanzania No. 24 Vol. 107 Dated 19th June, 2026
Printed by The Government Printer, Dodoma by Order of Government

GOVERNMENT NOTICE NO. 147 published on 19/6/2026

**THE CYBERCRIMES ACT,
(CAP. 443)**

ORDER

(Made under section 28)

THE CYBERCRIMES (PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE)
ORDER, 2026

Citation

1. This Order may be cited as the Cybercrimes
(Protection of Critical Information Infrastructure) Order,
2026.

Interpretation

2. In this Order, unless the context otherwise
requires-

Cap. 443

“Act” means the Cybercrimes Act;

“contact person” means a designated officer responsible for
regulatory liaison, incident reporting, compliance
coordination and day to day communication with
the Ministry regarding the critical information
infrastructure;

“critical information infrastructure” includes an asset,
device, computer system or network, whether
physical or virtual, which is vital to the United
Republic that its incapacitation affects national
security or the economy and social wellbeing of
citizens;

“data” includes databases, system logs, transaction records,
metadata, backups and any structured or
unstructured information processed or generated by
the critical information infrastructure;

- “Minister” means the Minister responsible for Information and Communication Technology;
“Ministry” means the Ministry responsible for Information and Communication Technology;
“operator” means a person or an entity that operates a critical information infrastructure; and
“owner” means a person or an entity that owns a critical information infrastructure.

Designation of
critical
information
infrastructure

3.-(1) The following computer systems are designated as critical information infrastructure:

- (a) National Information Communication Technology Broadband Backbone;
- (b) Submarines Cable Landing Stations;
- (c) National Internet Exchange Points;
- (d) Data Centres;
- (e) Public Telecommunication, Postal and Broadcasting Infrastructure Information Systems;
- (f) Government Centralised Management Information Systems;
- (g) Management Information Systems for National Security and Safety;
- (h) National Elections Management Information Systems;
- (i) National Social Security Management Information Systems;
- (j) Civil Aviation Management Information Systems;
- (k) Early Warning Management Information Systems;
- (l) National Banking and Financial Payment Management Information Systems;
- (m) Government Revenue Collection and Monitoring Management Information Systems;
- (n) National Identification and Registration Management Information Systems;
- (o) Railway Signaling, Communication and Freight Management Information Systems;

- (p) National Public Health Management Information Systems;
- (q) Energy and Public Utilities Management Information Systems;
- (r) Public Transport Management Information Systems;
- (s) Land Management Information Systems;
- (t) National Education Core Management Information Systems;
- (u) Mineral Resources Management Information Systems;
- (v) Food Supply System Management Information Systems;
- (w) Marine, Harbour or Port operation and Management Information Systems;
- (x) Emergency Services System Management Information Systems; and
- (y) Water Supply and Sewage Management Information Systems.

(2) The Minister may, upon consultation with the Ministry responsible for Information and Communication Technology of Zanzibar, add, alter or remove a computer system stated under subparagraph (1).

Registration of
critical
information
infrastructure

4.-(1) There shall be kept and maintained in the Ministry, a register of critical information infrastructure which shall include the following information:

- (a) relevant critical services provided by the owner;
- (b) relevant data and potential dependencies;
- (c) operators of the critical information infrastructure;
- (d) contact person;
- (e) asset inventory;
- (f) information on interconnected computer systems;
- (g) hosting solutions;
- (h) network architecture;
- (i) internet links supporting critical information infrastructure; and
- (j) any other relevant information as may be considered necessary.

(2) An owner of critical information infrastructure designated under paragraph 3 shall, within six months from the commencement of this Order, register a critical information infrastructure by filling in a form set out in the First Schedule and submit it to the Ministry.

Assessment of
information
systems

5.-(1) Every government institution and private entity shall, within six months from the commencement of this Order, conduct self-assessment on their information systems by using the checklist set out in the Second Schedule to determine if they are critical information infrastructure.

(2) After conducting self-assessment under subparagraph (1), the government institution or private entity shall submit a self-assessment report to the Ministry.

(3) The Ministry shall, upon receipt of the self-assessment report under subparagraph (2), evaluate the report and determine whether the system may be designated as critical information infrastructure or not.

(4) The Ministry shall, upon being satisfied with the report received under subparagraph (3), prepare an initial list of the system to be designated as a critical information infrastructure.

(5) The Ministry responsible for Information and Communication Technology of Zanzibar shall submit the list of critical information infrastructure to the Minister for designation.

Protection and
preservation

6.-(1) An owner shall be in charge of operating, protecting and preserving its critical information infrastructure.

(2) Subject to subparagraph (1), the owner shall, on quarterly basis, carry out a risk assessment analysis and submit business continuity plans to the Ministry.

Management
of critical
information
infrastructure

7. An owner shall be responsible for the management of critical information infrastructure.

8.-(1) Subject to the provisions of the Act and any other relevant laws, an owner shall-

Access, control
and transfer of
data

(a) take necessary steps for ensuring secure access, control and transfer of data related to critical information infrastructure; and

(b) host all data related to critical information infrastructure within the United Republic.

(2) An owner who intends to host its primary or secondary data related to critical information infrastructure outside the United Republic shall seek approval of the Minister.

Integrity and
authenticity of
data or
information

9. An owner shall ensure integrity and authenticity of data or information contained in critical information infrastructure.

Storage and
archiving of
data or
information

10. An owner or operator shall ensure storage and archiving of data or information relating to the critical information infrastructure in accordance with the Act and the relevant written laws.

Disaster
recovery plans

11.-(1) For the purposes of ensuring the continued availability, integrity, resilience and authenticity of critical information infrastructure, an owner shall ensure the availability of functional disaster recovery sites, risk management policy, backup procedures and restoration procedures.

(2) For the purposes of ensuring business continuity, the operator shall be in charge of operating and securing their infrastructure by carrying out risk assessment.

Audit and
inspection

12. For the purposes of critical information infrastructure protection compliance-

(a) the owner shall, within every six months from the date of registration of critical information infrastructure, conduct audit and inspection as part of internal operation and submit a report to the Ministry; and

(b) the Ministry shall carry out audits and inspection of critical information infrastructure

annually or at such higher frequency (interval)
in any particular case.

FIRST SCHEDULE

(Made under paragraph 4(1))

**APPLICATION FORM FOR THE REGISTRATION OF CRITICAL INFORMATION
INFRASTRUCTURE**

1. Sector:
The sector which critical information infrastructure belongs
to.....
2. Sector Lead:
Regulatory body that oversees the critical information infrastructure:
.....
3. Critical Information Infrastructure System Name:
(a) Name of designated critical information infrastructure system
.....
(b) Physical Address of critical information
infrastructure.....
4. Critical Information Infrastructure Functional Description:
Functional description of the designated Critical Information Infrastructure
system.....
5. Critical Information Infrastructure Owner(s):
Name of designated critical information infrastructure owner
.....
6. Critical Information Infrastructure Contact Details:
(a) Contact Name.....
(b) Designation.....
(c) Contact No..... Email Address.....
(d) Role.....
7. Other Particulars:
Any other particular as may be required
8. Other Remarks:
Critical information infrastructure processes or stores personal identifiable data:
Yes/No

I confirm that all the information I have given is correct and complete and I hereby
request to register the above Information Infrastructure as a Critical Information
Infrastructure.

Name:

Signature:

Position :.....

Date:

For Official Use Only:

Name:
Signature:
Position:
Date:

SECOND SCHEDULE

(Made Under Paragraph 5 (1))

**CHECKLIST FOR ASSESSING AN INFORMATION SYSTEM TO QUALIFY AS CRITICAL
INFORMATION INFRASTRUCTURE**

This assessment checklist covers various aspects of information system's security, reliability, and importance to the organization and the Nation at large to determine if it qualifies as critical information infrastructure. Mark the appropriate by putting (V) in the respective questions below:

S/N	CHECKLISTS ITEM	YES	NO
1	ORGANIZATIONAL IMPORTANCE		
	Core Operations		
	Is the information system essential for the core operations of the organization?		
	Does the system facilitate key company operations?		
	Financial Impact		
	Would its failure result in significant financial loss?		
	Does the system necessary to generate income?		
	Interdependencies		
	Are there any other procedures or systems that are dependent on it?		
	Is it a key component in a chain of critical systems?		
	Regulatory Requirements		
	Is there any legislative requirements that categorize this system as essential?		
	Does the system handle regulated data or functions?		
2	PUBLIC SAFETY AND SECURITY		
	Does the system support public safety services (e.g., emergency services, healthcare etc)?		
	Could its failure endanger public security or safety?		
	National Security		
	Is the system part of the national security infrastructure?		
	Would its compromise affect national defense or intelligence operations?		
3	TECHNICAL RESILIENCE		
	Physical Security		
	Are data centres and facilities housing the system physically secure?		
	Are there physical access controls and surveillance measures?		
	Cybersecurity		

	Is there comprehensive cybersecurity protection (e.g., firewalls, intrusion detection)?		
	Are there protection measures against cyber-attacks (e.g., DDoS, malware)?		
4	OPERATIONAL CONTINUITY		
	Redundancy		
	Are there redundant systems and failover mechanisms to ensure availability?		
	Are critical components duplicated across multiple locations?		
	Disaster Recovery		
	Is there a documented and regularly tested disaster recovery plan?		
	Are recovery time objectives (RTO) and recovery point objectives (RPO) metrics established and achievable?		
	Incident Response		
	Is there a robust incident response plan for cybersecurity and operational incidents?		
5	OPERATIONAL PERFORMANCE		
	Monitoring		
	Are there continuous monitoring systems for performance and availability?		
	Are performance metrics clearly defined and regularly reviewed?		
	Capacity Management		
	Is there a plan for managing and scaling system capacity?		
	Are usage patterns analyzed to anticipate future needs?		
	Service Level Agreements (SLAs)		
6	RISK MANAGEMENT		
	Risk Assessments		
	Are regular risk assessments conducted?		
	Are risks categorized and prioritized based on impact and likelihood?		
	Mitigation Strategies		
	Are there strategies and controls to mitigate identified risks?		
	Are high-priority risks addressed promptly and effectively?		
	Vulnerability Management		
7	GOVERNANCE AND COMPLIANCE		
	Policies and Procedures		
	Are there documented policies and procedures governing the system?		
	Are policies regularly reviewed and updated to reflect current threats and best practices?		
	Audits and Reviews		
	Are there regular internal and external audits of the system?		

	Are audit findings and recommendations promptly addressed?		
	Training and Awareness		
8	COMMUNICATION AND COORDINATION		
	Stakeholder Communication		
	Are there clear communication protocols for stakeholders regarding system status and incidents?		
	Are stakeholders regularly updated on system performance and security?		

	External Coordination		
	Is there coordination with external parties (vendors, partners) regarding system security and resilience?		
9	COMPLIANCE AND REGULATORY ADHERENCE		
	Legal Compliance		
	Is the system compliant with relevant laws and regulations (e.g., The Personal Data Protection Act, Cap.4, The Cybercrimes Act, Cap.443 and The e-Government Act, Cap.273)?		
	Are compliance requirements regularly reviewed and integrated into system management?		
	Industry Standards		
	Does the system adhere to industry-specific standards and best practices (e.g., TBS, ISO etc)?		
	Are certifications maintained and updated?		
10	RESILIENCE AND REDUNDANCY		
	Business Continuity		
	Are business continuity plans in place and regularly tested?		
	Is there a strategy for maintaining critical functions during an outage?		
	System Redundancy		
	Are there backup systems and data centers in geographically diverse locations?		

Dodoma,
22nd May, 2026

ANGELLAH JASMINE MBELWA KAIRUKI
*Minister for Communication and
Information Technology*