GOVERNMENT NOTICE No. 395 published on 3/08/2018

SOCIAL SECURITY (REGULATORY AUTHORITY) ACT
(CAP. 135)

GUIDELINES

(Made under section 5(1)(c))

THE SOCIAL SECURITY SCHEMES (SECURITY OF ELECTRONIC INFORMATION) GUIDELINES, 2018

ARRANGEMENT OF GUIDELINES

PART III
DATA PRIVACY

PART IV
ACCESS CONTROL

PART V
SECURITY IN APPLICATION DEVELOPMENT

PART VI
OUTSOURCING OF ELECTRONIC SERVICES

PART VII
INFORMATION AVAILABLE THROUGH MOBILE DEVICES AND WEBSITES

PART VIII
GENERAL PROVISIONS

GOVERNMENT NOTICE No. 395 published on 3/08/2018

SOCIAL SECURITY (REGULATORY AUTHORITY) ACT
(CAP. 135)

GUIDELINES

(Made under section 5(1)(c))

THE SOCIAL SECURITY SCHEMES (SECURITY OF ELECTRONIC INFORMATION) GUIDELINES, 2018

PART I
PRELIMINARY PROVISIONS

Citation

1. These Guidelines may be cited as the Social Security Schemes (Security of Electronic Information) Guidelines, 2018.

Application

2. These Guidelines shall apply to all schemes in Tanzania Mainland.

Interpretation

3. In these Guidelines, unless the context requires otherwise-

Cap. 135

"Act" means the Social Security (Regulatory Authority) Act;

"Authority" means the Social Security Regulatory Authority established under section 4 of the Act;

“Board” means the Board of Trustees established under the respective scheme’s laws;

“data privacy" means the right to maintain secrecy of personal information of a member;

“electronic information" means information that is stored or communicated digitally;

“ICT" means Information and Communication Technologies;

“information security" means the administrative and technical measures taken to ensure that data is only accessible by those who are entitled to use it, modified by those who are entitled to do so, and that information system can be

used by those who are entitled to use them;

mandatory scheme" means a compulsory scheme established by law and guaranteed by the Government to provide social security benefits to employees;

Cap. 306 "National Computer Emergency Response Team" means a computer emergency response team established under section 124 of the Electronic and Postal Communication Act;

"penetration test" means a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including operating systems, service and application flaws, improper configurations, and risky end-user behaviour, so as to validate the efficacy of defensive mechanisms, as well as end 'users' adherence to security policies;

"scheme" means the social security scheme and includes mandatory and supplementary schemes;

"security audit" means an evaluation of how secure an information system is;

"supplementary scheme" means a voluntary scheme chosen by the member to compliment benefit of any mandatory scheme.

Objectives of Guidelines

4.-(1) The general objective of these Guidelines shall be to guide the Board to ensure that mechanisms are put in place to manage information security risks.

(2) Without prejudice to sub paragraph (1), the Guidelines shall specifically aim at-

(a) preserving the privacy of member's personal data;

(b) ensuring availability of electronic systems; and

(c) preserving integrity of electronic information.

PART II

GOVERNANCE OF INFORMATION SECURITY

Adoption of framework for management

5. The Board shall issue a policy statement on the adoption of a framework for management of information security.

Inclusion of information security agenda

6. The Board shall, at least once a year during its Board meetings, include an agenda on information security.

Management of information

7. Management of information security shall be mandated to a specific officer within the organizational structure of the

security scheme.

Employee's awareness in information security

8. All employees involved in the creation, handling, processing and destruction of electronic data shall attend awareness sessions on trends in information security at least once a year.

Independent assurance

9.-(1) Independent assurance on information security shall be provided at least every three years and shall be provided as a result of a technical assessment

(2) For the purpose of this paragraph, "Independent assurance means technical assessment of security of information electronic through Information Systems Security Audit and a Network Penetration Test

Requirement to report

10. The Scheme shall report annually to the Authority on the security of members' data in a format to be prescribed by the Authority.

PART III
DATA PRIVACY

Privacy of personal data

11.-(1) Privacy of member's personal data shall be preserved throughout its life time with the scheme.

(2)Any information related to member's personal data shall be released only to persons authorized to access such information in accordance with the existing statutory requirements.

(3) The Board shall-

(a) put in place controls to ensure data privacy and integrity are preserved;

(b) limit information system access through remote access or on the schemes premises to-

(i) authorized users;

(ii) processes acting on behalf of authorized users;

(iii) devices (including other information systems); and

(iv) types of transactions and functions that authorized users are permitted to exercise.

PART IV
ACCESS CONTROL

Access control

12.-(1) Where information security breaches are

and incident reporting

suspected, there shall be incident handling and reporting mechanisms that are escalated internally up to the Board.

(2) The escalation may transmitted to the National Computer Emergency Response Team, depending on the severity of the incident.

(3) Escalation to the National Computer Emergency Response Team shall be in line with the Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2018.

PART V
SECURITY IN APPLICATION DEVELOPMENT

Documentation of in-house developed systems

13.-(1) All information systems developed in-house or developed specifically for the scheme to create, store or manipulate members' data shall have documented source code management procedures.

(2) All information systems developed in-house or developed specifically for the scheme must have documented security controls for access control, preservation of privacy and availability.

(3) All information systems developed shall have built-in validation mechanisms.

PART VI
OUTSOURCING OF ELECTRONIC SERVICES

Security for outsourced information services

14.-(1) Contracts for outsourced services shall include a requirement to adhere to secure practices including non-disclosure agreements.

(2) Where outsourced services involve exchange of information related to member's personal data or contribution, the Board shall submit a notice to outsource such services to the Authority together with controls for assurance of data privacy of the data that is given to outsourced service providers.

PART VII
INFORMATION AVAILABLE THROUGH MOBILE DEVICES AND WEBSITES

Mobile devices used for transaction

15. Mobile devices and systems used for transactions related to schemes' operations shall be equipped with sufficient controls to ensure security of any information stored on those devices.

Formal adoption of websites

16. The Board of Trustees shall formally adopt the websites, social network pages, electronic media forum or both, to be associated with official communication of schemes.

PART VIII
GENERAL PROVISIONS

Sanctions

17.-(1) Any scheme which contravenes the provisions of these Guidelines commits an act which constitutes "unsafe or unsound conduct" as provided in the Act, and such act shall be punishable in the manner provided in the Act.

(2) Notwithstanding the penalty imposed under sub paragraph (1), the Authority shall have the powers to-

(a) direct the scheme to comply with these Guidelines;

(b) propose disqualification of the Board of Trustees of schemes and Management of the schemes to the respective appointing Authority;

(c) suspend or disqualify the firm from conducting actuarial activities to the Schemes for a period as may be specified in the order;

(d) take any other necessary measures as the Authority may considers appropriate for the better implementation of these Guidelines.

Disapplication of Guidelines and savings

18.-(1) The Social Security Schemes (Security of Electronic Information) Guidelines, 2017 issued prior to the coming into effect of these Guidelines are hereby disapplied.

(2) Notwithstanding sub paragraph (1), anything done, action, claim or directive made pursuant to the (Security of Electronic Information) Guidelines, 2017 shall continue to have effect as if were made, issued or prepared under these Guidelines.

Dodoma
....., 2018

IRENE C. ISAKA
Director General