Telkom

Information Security Policy

TABLE OF CONTENTS

1 PURPOSE AND OBJECTIVES 3
2 APPLICABILITY AND SCOPE 3
3 CONTEXTUAL BACKGROUND 3
4 INFORMATION PROTECTION REQUIREMENTS 3
5 INFORMATION SECURITY MANAGEMENT 4
6 INFORMATION SECURITY MEASUREMENT 4
7 ROLES AND RESPONSIBILITIES 5
8 APPENDIX A: DEFINITIONS, ACRONYMS, REFERENCE DOCUMENTS, LAWS & REGULATIONS 6

1 PURPOSE AND OBJECTIVES

The Information Security Policy outlines the Board of Directors and Management's commitment to the protection of the Telkom SA SOC Limited (hereinafter referred to as "Telkom") information resources. The policy shall assist:

I. Telkom to effectively identify, manage, measure, and monitor potential Information Security risk exposures ensuring that information assets are protected against internal, external, deliberate, malicious, environmental, or accidental threats.

II. With the establishment of an effective organisational structure to govern Information Security for Telkom.

III. In outlining roles and responsibilities of stakeholders in Information Security management.

2 APPLICABILITY AND SCOPE

This policy applies to all Telkom employees, temporary employees, contractors, consultants, and associated third parties who have access or require access to Telkom's information assets and facilities relating to all forms of logical and physical access to information whether contained in hardcopy or electronic format.

3 CONTEXTUAL BACKGROUND

All information resources within Telkom, whether owned wholly or held in trust for, or on behalf of, customers, clients, subcontractors, or personnel, are defined as an asset. As such information is considered to have a value, and it shall be suitably protected.

4 INFORMATION PROTECTION REQUIREMENTS

The following is required when protecting information:

I. Confidentiality: Information shall be protected from unauthorised disclosure. This applies to information including intellectual capital, proprietary information, unclassified but sensitive information, customer and client records, and sensitive information subject to legislative or regulatory protection.

II. Integrity: There shall be assurance of the accuracy, completeness, and validity of information. Information shall be protected from unauthorised changes, erroneous modification, or illicit destruction, so that the integrity of the information is assured.

III. Availability: Information shall be available for delivery, storage and processing when and where needed (compromising neither its confidentiality nor its integrity) to support the operational, analytic, and decision-making processes to function effectively and profitably..

IV. Legislative and regulatory: Information protection shall meet legislative and regulatory requirements.

V. Commercial and contractual: Appropriate policies or controls shall be implemented where industry or commercial standards require compliance.

5 INFORMATION SECURITY MANAGEMENT

Information Security management refer to the planning, implementation and co-ordination of Telkom-wide measures aimed at protecting business information. It aims to address the information protection requirements highlighted above, as follows:

I. Information Security resources shall be made available to permit delivery of approved Information Security services, including technical security and qualified human resources.

II. A continuous Information Security risk assessment approach shall be followed where Information Security risks are identified, prioritised and treatment plans developed through creating and implementing effective security principles, standards, and procedures.

III. This policy is supported by Information Security Principles, documented separately and applied in the planning, design, build and operation of every information system used.

IV. The Information Security Policy and Information Security Principles are supported by Information Security standards. These dictate how specific Information Security areas shall be managed and configuration standards assist in establishing security in technical configurations.

V. Information Security procedures shall exist to support this policy, including delivery and operation of security systems, application systems and network patching and maintenance, access and identity management, and IT service continuity procedures which shall be actively managed and reported on to provide Information Security assurance.

VI. Suitable operational security measures shall be implemented and operated to prevent Information Security incidents from occurring, and ensure the appropriate detection, response, and correction of such events as dictated by the Information Security standards and procedures.

VII. Technical security measures shall include deployment and operational management of the security process, IT and network security systems and mechanisms to assure confidentiality, integrity, and availability of information resources as dictated by the Information Security standards.

VIII. Training and awareness on the value of information, and the appropriate protection of that information shall be made available to employees on an ongoing basis.

IX. Business Continuity Plans shall be developed, maintained, and tested to ensure that information is protected and available to deliver business functions.

6 INFORMATION SECURITY MEASUREMENT

I. Measurement and compliance: Where controls, as required by policy, standard and procedure quantifiable and reportable measures are implemented to manage Information Security. Such reports shall be regularly audited and reported on for compliance as part of a standard security assurance function.

II. Reporting of Information Security breaches: All actual or suspected security incidents affecting shall be reported to Corporate Information Security Governance (CISG) to be recorded and thoroughly investigated.

7 ROLES AND RESPONSIBILIES

7.1 Telkom Board of Directors

The Board of Directors is accountable for the governance of Information Security within and the approval of this policy.

7.2 Policy Owner

The owner of this policy is the IT Governance, who is accountable and responsible for updates to this policy.

7.3 Management

Management is responsible for identifying risks and the implementation of Information Security controls throughout the organisation, in line with this policy and any supporting principles, standards, and procedures. Telkom Information Security, Compliance, and IT Risk Forum.

The forum shall be responsible for facilitating the development, approval and implementation of appropriate Information Security policies, principles, standards and procedures which prescribe the relevant security controls and security assurance processes. The forum shall assist in the delivery of effective Information Security by maintaining a list of all current Information Security policies, standards, procedures, and guidelines.

7.4 Users

Telkom employees and other workers including consultants and contractors are responsible for ensuring that information assets are used only in proper pursuit of Telkom's business in accordance with Information Security policies, standards, and procedures, ensuring that information is not improperly disclosed, modified, or endangered and that access to Telkom's information resources is not made available to any unauthorised person. Users are responsible for reporting Information Security breaches and employees shall adhere to Information Security controls applicable their environment.

8 APPENDIX A: DEFINITIONS, ACRONYMS, REFERENCE DOCUMENTS, LAWS & REGULATIONS

8.1 Definitions

Definitions	Description
Business / Application / Information / Asset Owner	The Owner is accountable for ensuring that all risks that exist around an information asset are assessed and appropriately mitigated in favour of efficient, secure, and profitable business operation.
Cyber Security	Includes but is not limited to the protection of information and systems against adversarial (malicious or hostile) threats.
Information	Includes electronically generated data and written documents, pertaining to financial, technical, operational, governance and related and customer records.
Information Assets	Information in various forms, e.g., data stored on computers, transmitted over networks, printed, or written on paper, sent by fax, stored electronically, or discussed during telephone conversations.
Information Classification	The assignment of specific named levels of classification as defined within the Telkom Record Classification Policy, used to clearly identify value, significance, and necessary protective measures.
Information Resources	Includes but is not limited to the procedures, equipment, facilities, software, and data which are designed, built, operated, and maintained to collect, record, process, store, retrieve, display and transmit information. This includes data networks, servers, personal computers, and mobile computing devices, all end-user devices connected to Telkom's networks, such as storage media, printers, photo copiers, fax machines, supporting equipment, fall-back equipment, and back-up media, as well as computer logon codes.
Information System	An integrated set of components for collecting, storing, and processing data and for providing information, knowledge, and digital products.
Information Security	Includes but not limited to protection of information against unauthorised disclosure, transfer, modification, destruction, whether accidental, environmental, or other adversarial threats.
Management	Telkom Management implies employees that have the authority to implement Group Chief Executive Officer sanctioned management activities delivered on behalf of the Board either directly or through duly delegated Executive Committee actions implemented via the relevant governance council.
Security Policy	Any policy that contains function or area specific Information Security related requirements, created in support of the Information Security Policy, including Network Security Policy, Information Access Security Policy, Remote Access Security Policy, etc.

Definitions	Description
Users	Telkom employees and other workers including consultants and contractors.

8.2 Acronyms

Acronyms and Abbreviations	Description
Board	Telkom Board of Directors
CISG	Corporate Information Security Governance
EXCO	Executive Committee
ISO	International Organisation for Standardisation
IT	Information Technology
PCI DSS	Payment Card Industry Data Security Standard

8.3 Reference Documents

I. The ISF Standard of Good Practice for Information Security (SOGP)
II. King IV Code on Corporate Governance, 2016.
III. ISO 27001:2013 – Information Technology - Security Techniques – Information Security Management
IV. PCI DSS 3.2.1

8.4 Laws and Regulations

I. Electronic Communications and Transactions Act 25 of 2002
II. The Protection of Personal Information Act 4 of 2013