Information technology — Security techniques — Information security management systems — Requirements

ICS No: 35.030

TABLE OF CONTENTS

DATE OF PUBLICATION

This Gambian Standard was Gazetted under the authority of the Bureau on 2017

THE GAMBIA STANDARDS BUREAU

The Gambia Standards Bureau is a statutory Government specialized Agency established by The Gambia Standards Bureau Act 2010 to standardize products, methods, systems and for connected matters.

Hence, the Bureau is the sole National Standardization Body. As such, it has been a member of International Standardization Bodies such as the International Organization for Standardization (ISO) since 2011, International Electrotechnical Commission (IEC), the Standards and Metrology Institute for Islamic Countries (SMIIC) from 2012 and ASTM International in 2017.

The objectives of the Bureau, as specified in its Act, are to: establish and promulgate standards for imported and locally-produced goods; facilitate domestic and international trade; foster and promote standards both for industrial efficiency and advancing economic development; promote the health and safety of consumers; enhance international cooperation in relation to standards and standardization. The National Quality Policy details the responsibilities of the Bureau in Standardization, Metrology and Conformity Assessment services in Testing, Inspection and Certification.

Therefore, the functions, of the Bureau are to define, prepare, publish, modify or amend Standards Specifications as well information-dissemination of standards. In addition to providing Testing, Inspection and Certification services for goods, systems and processes independently or in relation to conformity with its Standards Mark, the Bureau also conducts training and research. In Metrology, the Bureau serves as the custodian of primary national reference measurement standards through its National Metrology Laboratories and conducts calibration of measurement devices and physical standards.

The development of Gambian Standards (GAMS) is carried out by the Bureau through Technical Committees composed of a balanced representation of stakeholders, as may be appropriate to the subject in question. The Bureau ensures that Standards are developed in accordance with the *ISO_IEC_Guide_21-1_2005: Regional or National adoption of International Standards and other International deliverables* and the *World Trade Organization Code of good practice for the preparation, adoption and application of standards*. To the greatest extent possible, Gambian Standards are aligned to or are adoptions of relevant international standards.

For further information on and copies of Gambian Standards, please contact The Gambia Standards Bureau.

TECHNICAL COMMITTEE RESPONSIBLE: Management systems

The Management systems TC developed this Quality management system requirements. The TC was set up in 2016 and began the work of development of standards in the field of Management systems.

The Management systems TC consists of representatives from the following Institutions/Organizations:

- Consumer Protection Association of The Gambia
- The University of The Gambia
- Food Safety and Quality Authority
- Gambia Chamber of Commerce and Industry
- Department of Health Services
- Gambia Competition and Consumer Protection Commission
- National Water and Electricity Company
- Management Development Institute
- Ministry of Energy and Petroleum

The Gambia Standards Bureau is the Secretariat and Secretary to the Management Systems Technical committee.

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives,Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 27001 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

1 Scope

This International Standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations). This International Standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.

The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

NOTE 1: References to 'business' in this International Standard should be interpreted broadly to mean those activities that are core to the purposes for the organization's existence.

NOTE 2: ISO/IEC 17799 provides implementation guidance that can be used when designing controls.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*