EDC6 (1938) DTZS
ISO/IEC 24767-1:2008

DRAFT TANZANIA STANDARD

(Draft for comments only)

Information technology — Home network security — Part 1: Security requirements

TANZANIA BUREAU OF STANDARDS

First Edition 2022

1 National Foreword

This draft Tanzania Standard is being prepared by the Telecommunications and Information Technology Technical Committee, under the supervision of the Electrotechnical divisional standards committee (EDC)

This draft Tanzania Standard is an adoption of the International Standard **ISO/IEC 24767-1:**2008 Information technology — Home network security — Part 1: Security requirements, which has been prepared by the International Electrotechnical Commission

2 Terminology and conventions

Some terminologies and certain conventions are not identical with those used in Tanzania standards; attention is drawn especially to the following: -

1) The comma has been used as a decimal marker for metric dimensions. In Tanzania Standards, it is current practice to use “full point” on the baseline as the decimal marker.

2) Where the words “International Standard(s)” appear, referring to this standard they should read “Tanzania Standard(s)”.

ISO/IEC 24767-1

Edition 1.0 2008-09

INTERNATIONAL STANDARD

Information technology – Home network security –
Part 1: Security requirements

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE K

ICS 35.200

ISBN 978-2-88910-837-4

CONTENTS

INFORMATION TECHNOLOGY – HOME NETWORK SECURITY –

Part 1: Security requirements

FOREWORD

1) ISO (International Organization for Standardization) and IEC (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. Their preparation is entrusted to technical committees; any ISO and IEC member body interested in the subject dealt with may participate in this preparatory work. International governmental and non-governmental organizations liaising with ISO and IEC also participate in this preparation.

2) In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. 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.

3) The formal decisions or agreements of IEC and ISO on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC and ISO member bodies.

4) IEC, ISO and ISO/IEC publications have the form of recommendations for international use and are accepted by IEC and ISO member bodies in that sense. While all reasonable efforts are made to ensure that the technical content of IEC, ISO and ISO/IEC publications is accurate, IEC or ISO cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.

5) In order to promote international uniformity, IEC and ISO member bodies undertake to apply IEC, ISO and ISO/IEC publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any ISO/IEC publication and the corresponding national or regional publication should be clearly indicated in the latter.

6) ISO and IEC provide no marking procedure to indicate their approval and cannot be rendered responsible for any equipment declared to be in conformity with an ISO/IEC publication.

7) All users should ensure that they have the latest edition of this publication.

8) No liability shall attach to IEC or ISO or its directors, employees, servants or agents including individual experts and members of their technical committees and IEC or ISO member bodies for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication of, use of, or reliance upon, this ISO/IEC publication or any other IEC, ISO or ISO/IEC publications.

9) Attention is drawn to the normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.

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

International Standard ISO/IEC 24767- 1 was prepared by subcommittee 25: Interconnection of information technology equipment, of ISO/IEC joint technical committee 1: Information technology.

The list of all currently available parts of the ISO/IEC 24767 series, under the general title *Information technology – Home network security*, can be found on the IEC web site.

This International Standard has been approved by vote of the member bodies, and the voting results may be obtained from the address given on the second title page.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

INFORMATION TECHNOLOGY – HOME NETWORK SECURITY –

Part 1: Security requirements

1 Scope

This part of ISO/IEC 24767 specifies home network security requirements that may come from inside or outside a home. It serves as a foundation for the development of security services against threats affecting the home environment.

The discussions about security requirements in this standard are presented in a relatively informal manner. Although many of the items discussed here are expected to guide the design of security mechanisms applied either inside home networks or through the Internet, they are not considered formal requirements.

Various devices are connected to the home network; see Figure 1. The devices of the “living network”, the devices for “A/V entertainment” and the devices for “informational applications” provide different features and performance. This standard provides means to analyse the risks for each networked device and to define its specific “security requirements”.

2 Terms, definitions and abbreviations

2.1 Terms and definitions

For the purpose of this document the following definitions apply.

2.1.1
brown goods
A/V devices that are mainly used for entertainment, for example, television or DVD recorder

2.1.2
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities or processes

2.1.3
data authentication
service used to ensure that the source of the data claimed by a party to a communication is correctly verified

2.1.4
data integrity
property that data has not been altered or destroyed in an unauthorized manner

2.1.5
user authentication
service used to ensure that the identity claimed by a party to a communication is correctly verified, whereas an authorization service ensures that the identified and authenticated party is entitled to access a particular device or application on the home network

2.1.6
white goods
appliances that are used for daily life, for example, air conditioner, refrigerator and so on