International Standard

ISO/IEC 7184

Office equipment — Security requirements for hard copy devices (HCDs) — Part 1: Definition of the basic requirements

Équipement de bureau — Exigences de sécurité pour les appareils de reprographie (HCD) — Partie 1: Définition des exigences de base

First edition
2024-02

Reference number
ISO/IEC 7184:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Requirements **4**
4.1 Security functional requirements 4
4.1.1 Overview 4
4.1.2 Identification and authentication 4
4.1.3 Security management 5
4.1.4 Software update 6
4.1.5 Field-replaceable nonvolatile storage data protection 6
4.1.6 Internet communication data protection 7
4.1.7 PSTN and network separation 7
4.2 Security assurance requirement 7
4.2.1 Overview 7
4.2.2 Configuration management 8
4.2.3 Operational environment 8
4.2.4 Flaw remediation 8
4.3 Vulnerability assessment 9
4.3.1 Overview 9
4.3.2 Verification by vulnerability scanners 9
4.3.3 Closure of unused TCP/UDP ports 9
4.3.4 Closure of debug ports 9
Bibliography **10**

© ISO/IEC 2024 – All rights reserved

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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had no*t* received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 28, *Office equipment*.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Introduction

The need for a secure working environment is increasing with the progress and spread of information and communications technology.

In particular, there are high security needs in the office environment where company information and customer information are handled.

With hard copy device (HCD) office equipment, it is common practice for many manufacturers to acquire common criteria (CC) certification and demonstrate to customers that they meet the Protection Profile, which defines the security requirements, environment, and so on required for HCD product areas.

While CC certification is a standard that guarantees relatively high security functionality, there is no indicator that shows the level of security functionality for models other than CC certified models. This causes confusion when selecting a model that has appropriate security functionality for use as office equipment and not intended for home use.

If HCDs are used in the office without proper model selection, security risks are introduced.

It is necessary to establish an index that can judge whether or not the appropriate security functionality is satisfied as office equipment.

Among them, this time, as office equipment, an index was created that defines the basic security requirements for small office, home office users.

© ISO/IEC 2024 – All rights reserved

Office equipment — Security requirements for hard copy devices (HCDs) — Part 1: Definition of the basic requirements

1 Scope

This document defines basic security requirements for the protection of hard copy devices (HCDs) including identification and authentication, security management, software update, field-replaceable nonvolatile storage data protection, network data protection and public switched telephone network (PSTN) fax-network separation.

It can be applied to office equipment with network functions including printers, scanners, fax machines, digital copiers, and digital multi-function machines, specifically for small office and home office users.

This document assumes a small, private information processing environment in which most elements of security are provided by the physical environment. In such an environment is assumed to be physically and logically protected from threats originating from outside of that environment, typically by limiting physical access to the HCD and connecting it to a LAN that is protected from the public Internet. A small office or home office would be a typical example of this environment.

Please note that the requirements outlined in this document are not intended to replace the existing Common Criteria Certification for hardcopy devices which ensure the minimum-security requirements for enterprise environment. For example, aspects being required in Common Criteria Certification such as audit data generation, self-test capabilities, and protection of key material are not adequately addressed.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
hard copy device
HCD
printer, scanner, fax machine, digital copier, or digital multifunction device

3.2
security setting
setting that is designed to affect device security functionality

Note 1 to entry: Security settings include settings related to network connection and time.

3.3
user identifier
character string or pattern that is used by a data processing system to identify a user

Note 1 to entry: Some devices support different categories of user including *administrator* (3.5) and *normal user* (3.6).

© ISO/IEC 2024 – All rights reserved