International Standard

ISO/IEC 7184

First edition
2024-02

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

Reference number
ISO/IEC 7184:2024(en)

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

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 not 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.

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.

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).

[SOURCE: ISO/IEC 20944-1:2013, 3.11.4.17, modified — Note 1 to entry was added.]

3.4
authentication
action to prove the identity of the *administrator* (3.5) or *normal user* (3.6)

3.5
administrator
user with authority to manage some portion or all of the *hard copy device (HCD)* (3.1) and whose actions may affect the HCD security policy

3.6
normal user
user with authority to use a device but not to configure or change *security settings* (3.2)

3.7
data integrity
property that signifies that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989, 3.3.21]

3.8
digital signature
digest generated from data using a hash function and encrypted with a private key

Note 1 to entry: *Data integrity* (3.7) can be verified with digital signatures by applying public key cryptography.

3.9
field-replaceable nonvolatile storage device
nonvolatile storage device that can be swapped in the field to repair a malfunction

3.10
wear levelling
distribution of the writing locations of memory storage with a limited number of write cycles to increase its life

Note 1 to entry: Storage element of flash memory such as solid-state drives generally have a limit to the number of rewrites. To maximize the life of these devices, the writing positions are dispersed so that the writing is not concentrated on a specific storage element. This distributed technology is called wear levelling. Once data would be deleted logically, it would be difficult to restore data because the write positions are distributed by the controller.

3.11
vulnerability
weaknesses that compromise security or operation of a system

Note 1 to entry: There could be a case that security flaws in design or implementation are referred as vulnerabilities. Besides software vulnerabilities in some cases an incomplete state of setting security options sometimes are referred to as being vulnerable.

3.12
threat
factors that pose a security risk

Note 1 to entry: Security risks arise when threats and vulnerabilities combine.

3.13
firmware
hardware that contains a computer program or data that cannot be changed in its user environment

Note 1 to entry: The computer program and data contained in firmware are classified as software; the circuitry containing the computer program and data is classified as hardware.

[SOURCE: ISO 10795:2019, 3.105]

3.14
firewall
type of security barrier placed between network environments — consisting of a dedicated device or a composite of several components and techniques — through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass

[SOURCE: ISO/IEC 27033-1:2015, 3.12]

3.15
configuration management system
system for configuring electronic device software, *firmware* (3.13) and hardware including version control of each component part

3.16
security function
functions which are implemented in the *hard copy device (HCD)* (3.1) as countermeasures to risks for important assets residing in the HCD

Note 1 to entry: The security functions should be enabled or configured according to *security settings* (3.2) specified with security management function.

3.17
administrator rights
authority to modify device settings including *security settings* (3.2)

Note 1 to entry: Administrator rights may require a *user identifier* (3.3) and password or may require only a password depending on the product specification.

3.18
network function
network service function using Internet protocol (IP) for the internet layer and transmission control protocol (TCP) and / or user datagram protocol (UDP) for the transport layer

Note 1 to entry: In this document, the network interface layer such as a wired local area network (LAN) or wireless LAN need not be considered.

3.19
image overwrite function
function to write some meaningless data onto a medium so that residual data cannot be retrieved

Note 1 to entry: This technique is often used for clearing residual image data stored in electron medium such as hard disk driver (HDD).

3.20
logical deletion function
technique for clearing data stored in a logical file system

Note 1 to entry: The function erases indices to the data stored and removed from the file system so that residual image data cannot be accessed through the file system.

3.21
credential stuffing
type of cyberattack in which the attacker collects stolen account credentials

3.22
resource exhaustion
computer security exploits that crash, hang, or otherwise interfere with the targeted program or system

3.23
solid state drive
storage device that uses integrated circuit assemblies, typically flash memory, to store data persistently

Note 1 to entry: In general, solid state drive uses *wear levelling* (3.10) technique when rewriting data.

4 Requirements

4.1 Security functional requirements

4.1.1 Overview

The security functional requirements specified in this document are as follows. Some requirements are mandatory only where the applicable function is included in the HCD:

— identification and authentication,

— security management,

— software update,

— field-replaceable nonvolatile storage data protection,

— internet communication data protection, and

— PSTN and network separation.

4.1.2 Identification and authentication

4.1.2.1 Authentication of administrator

4.1.2.1.1 Background

A security risk for an HCD is that there is a possibility that an unauthorized third party accesses security settings and take control of the system or otherwise tamper with it.

4.1.2.1.2 Requirements

HCDs shall have a function to require administrator rights when accessing security settings remotely. Depending on the implementation of the function, there could be cases that the function requires both user identifier and password or only a password; the capability to uniquely identify the administrator is not required.

4.1.2.2 Change of default password

4.1.2.2.1 Background

A security risk for an HCD is that unauthorized third parties easily estimate the administrator ID (where used) and password to access and change the security settings and take control of the system or otherwise tamper with it.

4.1.2.2.2 Requirements

HCDs that support modification of security settings remotely shall have a function that allows an administrator to change the passcode used to gain administrator rights.

HCDs shall have a function that prompts the user to change the default passcode when using the device for the first time, or something equivalent to this, for example:

— user guidance states that the passcode should be changed from the initial value;

— different passcodes are assigned for each individual device.

The passcode may be just password, or user identifier and password depending on the authentication method used to gain administrator rights.

This requirement is applied only for the HCD which manages passcodes in itself. If the HCD does not manage the passcodes and if the HCD uses authentication means other than a passcode which is entered manually (digital signatures, etc.), or an external authentication server, this requirement is not applied.

4.1.2.3 Authentication failures

4.1.2.3.1 Background

The security risk for an HCD is that the administrator ID (if used) and password will be discovered through trial and error.

4.1.2.3.2 Requirements

If the HCD has authentication capabilities via a network interface, it shall have a mechanism available which makes brute force attacks on authentication mechanisms via network interface impracticable.

EXAMPLE 1 HCD has a limitation on the number of authentication attempts within a certain time interval. It also uses increasing time intervals between attempts.

EXAMPLE 2 HCD is able to lock an account or to delay additional authentication attempts after a limited number of failed authentication attempts after a limited number of failed authentication attempts.

This requirement addresses attacks that perform credential stuffing or exhaust an entire key-space. It is important that these types of attacks are detected by the HCD and defended against, whilst guarding against a related threat of resource exhaustion and denial of service attacks.

4.1.3 Security management

4.1.3.1 Security settings management

4.1.3.1.1 Background

A security risk for HCDs is that there is a possibility that unauthorized third parties change the security settings of the HCD and eliminate the normal security feature and leak or modify data or otherwise tamper with it.

4.1.3.1.2 Requirements

Remote setting and changing of security settings shall be restricted to authorized administrators.

4.1.3.2 Initialization of security settings

4.1.3.2.1 Background

A security risk for HCDs is that when returning, transferring or disposing of a device, attackers might read the security configuration information and carry out unauthorized access to the user's network based on this information. This could cause leakage of or tampering with user information.

4.1.3.2.2 Requirements

HCDs shall have a function to restore security settings to factory defaults or purge security settings values when returning, transferring, or disposing of an HCD. Where this initialization operation is performed via the network, it shall require administrator rights.

If initialization via the network is realized by a management tool on a PC, the management tool should have a function to prompt information, e.g. passcode to authenticate as an administrator.

4.1.4 Software update

4.1.4.1 Background

A security risk for HCDs is that a vulnerability in the software is discovered by an attacker who exploits this to take control of the device or tamper with it. It is therefore, important that the user is able to identify the current version of the software.

If the current version of the software cannot be confirmed, the administrator cannot understand the vulnerabilities inherent in the device.

Without the software update function, if a vulnerability is discovered, it cannot be fixed.

If a software update is tampered by a malicious attacker, it could cause a risk of attack such as compromising the data in the HCD or the network environment in where the HCD is deployed.

4.1.4.2 Requirements

HCDs shall have the ability to show the current version of the software.

HCDs shall have the ability to update the device software. Update operation via the network shall require administrator rights. The manufacturer may provide an update service such as automated remote update service, update service by a service person on behalf of an administrator.

HCDs shall have the ability to verify the integrity of the software to be installed before updating. If the verification of the integrity of the software fails, the device shall stop updating and where appropriate provide feedback to the user.

A digital signature may be used as a means of verifying the integrity and the authenticity of the software updates.

4.1.5 Field-replaceable nonvolatile storage data protection

4.1.5.1 Background

A security risk for HCDs is the possibility that an attacker removes the field-replaceable nonvolatile storage device from the HCD and reads the data in the field-replaceable nonvolatile storage device using, for example, a PC when the HCD is returned, transferred or otherwise disposed of.

4.1.5.2 Requirements

If the HCD has a field-replaceable nonvolatile storage device, it shall have a function to make the user-supplied data in the device unavailable by setting or operation. If the setting or operation is performed via the network, it shall be restricted to the administrator only.

This requirement applies to hard disk drives (HDDs) and solid state drives (SSDs) and does not apply to recording media connected via an external interface such as a USB memory or SD memory card. This requirement is not applied to any nonvolatile storage device which is not field replaceable.

Techniques to make the user data unavailable include:

— encryption of data on the storage device, or

— purging the data from the storage device.

For HDDs, an image overwrite function may be used as the technique to purge the data and for SSDs which have a wear levelling function, a logical deletion function may be used as the technique of purging the data.

The setting or operation for making user data unavailable may be done by a service person who has obtained the permission from the administrator.

4.1.6 Internet communication data protection

4.1.6.1 Background

A security risk for HCDs is that there is a possibility that a malicious user eavesdrops or modify the network data in the external communication path.

4.1.6.2 Requirement

HCDs with a network communication function that operates via the Internet shall have an encrypted communication function. If the device doesn't implement any protocols which are expected to communicate with the server on the Internet, this encrypted communication function is not required.

NOTE This requirement mentions an encrypted communication function at the internet layer, and does not require the protocol used for wireless LAN.

The manufacturer shall publish details of the encrypted communication method (including its version) used in the encrypted communication function.

4.1.7 PSTN and network separation

4.1.7.1 Background

If the fax and network are not separated, an attacker could break into a protected network environment via a PSTN fax modem. An attacker could obtain or modify user's data with unauthorized access that bypasses such firewalls or other external protections.

4.1.7.2 Requirements

If the HCD has a PSTN fax function, the HCD shall not have PSTN fax and network relay function.

4.2 Security assurance requirement

4.2.1 Overview

This document defines the security assurance requirements as follows:

— configuration management,

— operational environment, and

— flaw remediation.

4.2.2 Configuration management

4.2.2.1 Background

If the software components of an HCD are not configured by the appropriate version control, there is a concern that sufficient countermeasures against vulnerabilities will not be taken.

4.2.2.2 Requirements

HCDs shall be developed under a configuration management system, and an HCD and parts thereof shall be identified uniquely by configuration management.

4.2.3 Operational environment

4.2.3.1 Background

If the HCD is directly connected to the internet, the HCD is exposed to the threat of unauthorized access by an external attacker. In order to remove such threats, it is important to use it in a network protected from the outside, such as installing a firewall.

4.2.3.2 Requirements

The HCD information which is provided to the customer shall encourage the customer to use the HCD within a network that is protected from external attacks, for example by a suitably configured firewall.

4.2.4 Flaw remediation

4.2.4.1 Inquiry window

4.2.4.1.1 Background

If there is no vulnerability report and inquiry window, there is a concern that countermeasures against vulnerabilities will be delayed.

4.2.4.1.2 Requirements

The manufacturer of the HCD shall provide a means that users can report and inquire about suspicious vulnerabilities.

4.2.4.2 Providing software

4.2.4.2.1 Background

If there is no system to provide amended software when vulnerabilities are identified, the customer cannot take countermeasures. There is a possibility that using the HCD in an insecure state leads to leakage of information.

If the customer does not use the HCD with the amended software, there is a possibility that using the HCD in an insecure state leads to such leakage of information.

4.2.4.2.2 Requirements

The manufacturer of the HCD shall have a system to provide amended software when a vulnerability is found.

The manufacturer of the HCD shall make an announcement encouraging the use of the secure version of the software to the customer.