INTERNATIONAL STANDARD

# ISO/IEC 19678

First edition
2015-05-01

# Information Technology — BIOS Protection Guidelines

*Technologies de l'information — Lignes directrices de protection BIOS*

Reference number
ISO/IEC 19678:2015(E)

## COPYRIGHT PROTECTED DOCUMENT



ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

# Contents

Page

Foreword ..... v
Introduction ..... vi
1 Scope ..... 1
2 Conformance ..... 1
3 Normative references ..... 2
4 Terms and definitions ..... 2
5 Symbols (and abbreviated terms) ..... 3
6 Background ..... 4
6.1 System BIOS ..... 4
6.2 Role of System BIOS in the Boot Process ..... 5
6.3 Updating the System BIOS ..... 8
6.4 Importance of BIOS Integrity ..... 8
6.5 Threats to the System BIOS ..... 9
7 Threat Mitigation ..... 10
Bibliography ..... 14

# 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.

*Note: ITTF will provide the document number needed below*

ISO/IEC 19678 was prepared by the U.S. National Institute of Standards and Technology from NIST SP 800-147, BIOS Protection Guidelines. NIST SP 800-147 was reformatted in accordance with ISO/IEC Directives, Part 2, while maintaining the technical content of the NIST publication (available at http://csrc.nist.gov/publications/nistpubs/800-147/NIST-SP800-147-April2011.pdf). The resulting standard was adopted under a special “fast-track procedure”, by Joint Technical Committee ISO/IEC JTC 1, *Information technology,* in parallel with its approval by the national bodies of ISO and IEC.

# Introduction

Modern computers rely on fundamental system firmware, commonly known as the system Basic Input/Output System (BIOS), to facilitate the hardware initialization process and transition control to the operating system. The BIOS is typically developed by both original equipment manufacturers (OEMs) and independent BIOS vendors, and is distributed to end-users by motherboard or computer manufacturers. Manufacturers frequently update system firmware to fix bugs, patch vulnerabilities, and support new hardware. This International Standard provides security requirements and guidance for preventing the unauthorized modification of BIOS firmware on PC client systems.

Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on an organization—either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware). The move from conventional BIOS implementations to implementations based on the Unified Extensible Firmware Interface (UEFI) may make it easier for malware to target the BIOS in a widespread fashion, as these BIOS implementations are based on a common specification.

This International Standard focuses on current and future x86 and x64 desktop and laptop systems, although the controls and procedures could potentially apply to any system design. Likewise, although the guide is oriented toward enterprise-class platforms, the necessary technologies are expected to migrate to consumer-grade systems over time. The security requirements do not attempt to prevent installation of unauthentic BIOSs through the supply chain, by physical replacement of the BIOS chip, or through secure local update procedures.

The intended audience for this International Standard includes BIOS and platform vendors, and information system security professionals who are responsible for managing the endpoint platforms' security, secure boot processes, and hardware security modules. The material may also be of use when developing enterprise-wide procurement strategies and deployment.

The material in this International Standard is technically oriented, and it is assumed that readers have at least a basic understanding of system and network security. The International Standard provides background information to help such readers understand the topics that are discussed. Readers are encouraged to take advantage of other resources (including those listed in this International Standard) for more detailed information.

# Information Technology— BIOS Protection Guidelines

## 1 Scope

This International Standard provides requirements and guidelines for preventing the unauthorized modification of *Basic Input/Output System (BIOS)* firmware on PC client systems. Unauthorized modification of BIOS firmware by malicious software constitutes a significant threat because of the BIOS's unique and privileged position within the PC architecture. A malicious BIOS modification could be part of a sophisticated, targeted attack on an organization —either a permanent denial of service (if the BIOS is corrupted) or a persistent malware presence (if the BIOS is implanted with malware).

As used in this publication, the term BIOS refers to conventional BIOS, *Extensible Firmware Interface (EFI)* BIOS, and *Unified Extensible Firmware Interface (UEFI)* BIOS. This International Standard applies to system BIOS firmware (e.g., conventional BIOS or UEFI BIOS) stored in the system flash memory of computer systems, including portions that may be formatted as Option ROMs. However, it does not apply to Option ROMs, UEFI drivers, and firmware stored elsewhere in a computer system.

Subclause 7.2 provides platform vendors with requirements for a secure BIOS update process. Additionally, subclause 7.3 provides guidelines for managing the BIOS in an operational environment.

While this International Standard focuses on current and future x86 and x64 client platforms, the controls and procedures are independent of any particular system design.

## 2 Conformance

The following terms are used in this standard to indicate mandatory requirements, recommended options, or permissible actions.

- The terms "shall" and "shall not" indicate requirements to be followed strictly in order to conform to this standard and from which no deviation is permitted.
- The terms "should" and "should not" indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is discouraged but not prohibited.
- The terms "may" and "need not" indicate a course of action permissible within the limits of this standard.

An implementation is conformant to this standard if it implements the requirements specified in subclause 7.2.

## 3 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.

FIPS 186-4, *Digital Signature Standard.* July 2013.

NIST SP 800-89, *Recommendation for Obtaining Assurances for Digital Signature Applications.* November 2006.

NIST SP 800-131A, *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. January 2011.