ICS 35.030
CCS L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 29244-2024

Replacing GB/T 29244-2012

Cybersecurity technology - Security specification for office devices

网络安全技术 办公设备安全规范

Issued on: September 29, 2024 **Implemented on: April 1, 2025**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

2 Normative references

Three documents are cited: GB/T 18336, Information technology - Security techniques - Evaluation criteria for IT security; GB/T 25069, Information security technology - Terminology; and GB/T 29829, Information security technology - Functionality and interface specification of cryptographic support platform for trusted computing.

Dated references apply in the cited edition only; undated references apply in their latest edition, including all amendments.

3 Terms and definitions

The terms defined in GB/T 18336 and GB/T 25069 apply, together with the eight terms below.

3.1 office device: device used to produce or process electronic or other media documents.
Note: office devices are mainly devices having one or more of the printing, scanning, fax and copying functions.

3.2 administrator: user authorised to manage some or all parts of the office device.

3.3 user: entity, a person or an information technology entity, that operates the office device

or interacts with it.

3.4 user data: data created by the user or for the user that does not affect the operation of the security functions of the office device. Note: user data includes user document data and user function data.

3.5 non-volatile storage: storage whose stored data is not lost when the power is switched off. Note: non-volatile storage mainly includes built-in or external hard disks, universal serial bus (USB) drives, secure digital (SD) cards and flash memory.

3.6 firmware: programs that implement interface communication, security functions, data parsing, image processing and engine control of the office device.

3.7 master control chip: integrated circuit chip, or set of chips, responsible for data parsing, image processing, job management and control of the print head, and outputting binary image data directly.

3.8 data control board: circuit board built into the office device that carries the master control chip and is responsible for the data control functions. Note: the data control functions include data communication, job allocation and management, job data parsing, image processing of print, copy and scan data, and output control of the binary image data.

4 Abbreviations

IP, Internet Protocol; MAC, Media Access Control; PIN, Personal Identification Number; SNMP, Simple Network Management Protocol.

5 General

The security technical requirements for office devices are made of security function requirements and security assurance requirements. The security function requirements state the security functions the device is to have. The security assurance requirements state the security measures the device provider is to take during the design, development, production, delivery, operation, maintenance and supply chain management of the device.

The document divides the security level of office devices into a basic level and an enhanced level. The strength of the security functions and the height of the security assurance requirements are the basis of that division. The grading of the security technical requirements follows Annex A and the grading of the assessment methods follows Annex B.

6.1 Security function requirements

6.1.1 Identification and authentication. The user identity is to be identified, and authenticated when device functions and security functions are performed. Session timeout locking is to be supported, together with a settable maximum number of authentication failures beyond which authentication by the user is restricted for a period or the account is

locked. Where a default password exists, the user is to be allowed to change it and is to be prompted to do so.

6.1.2 Access control. Administrators and ordinary users are to be given the least access rights needed for their own tasks; authorisation management is to let the administrator grant rights to ordinary users; access to device functions and to user data is to be granted or refused according to an access control policy; an IP or MAC allow list is to be provided; execution of jobs through a PIN should be supported, with the job locked once the set maximum number of PIN failures is exceeded, and with a deletion mechanism applied when the device is switched off and restarted.

6.1.3 Firmware security. A firmware update management function is to be provided, the update being performed by the administrator where one exists and otherwise only after the separate consent of the user. Integrity and authenticity are to be verified before the update by digital signature, hash operation or an equivalent means, and the update stopped at once if verification fails. The firmware is not to contain malicious programs. Integrity and authenticity are to be checked automatically at start-up and work stopped at once if an anomaly is found. Where trusted verification is done by a trusted cryptographic module, that module is to meet GB/T 29829.

6.1.4 Log recording and auditing. Audit records are to be produced for the opening and closing of the audit function, the start or completion of device functions, use of the identification or authentication mechanism, changes of system time, firmware updates, replacement of chipped consumables, job data including but not limited to page and copy counts, and other events related to system security or defined as auditable. Each record is to carry at least the date and time of the event, the event type, the user identity and the result. Export of the records, for instance as an electronic file or a printed information report, is to be supported, the records are to be protected against unauthorised deletion, and, where no interface for sending records is provided, they are to be kept on the device for not less than six months.

6.1.5 User data security. User document data and the related temporary and cache files in the corresponding modules and in the driver are to be deleted automatically once the job is finished; measures are to ensure that a user can act only on their own document data; user data is not to be stored in the consumable chip, statistics on consumable use excepted; stored logs and configuration data are to be protected by measures including but not limited to encryption and integrity checking; where a fault or an error occurs and the user takes no action within a set time, user document data is to be deleted once the device returns to normal; automatic and manual clearing of residual information on consumables is to be provided.

6.1.6 Communication security. The device is to withstand common network attacks; ports, services and protocols unrelated to its functions are to be closed under the least authorisation principle; no covert channel is to exist; a function for closing ports, services

and protocols is to be provided; the connection is to be terminated automatically after a prescribed silent period; a secure SNMP protocol is to be used by default; the confidentiality, integrity and availability of the communicated data are to be protected; the device and the driver are to recognise each other before job data is transferred; where a wireless communication module is present, a function to close it is to be provided and it is to be off by default, the note listing wireless local area network, Bluetooth and infrared modules among others; network sharing and remote management, where present, are likewise to be closable and off by default; non-repudiation should be provided.

6.1.7 Non-volatile storage security. Functions are to be provided for checking the integrity of the user data held in non-volatile storage and for deleting it. Where a built-in removable non-volatile memory exists, it is to use a public data storage structure and exchange data with its control system through a public protocol; the note names the file allocation table (FAT) and the extended file system (EXT) as public structures and the integrated drive electronics (IDE) interface, serial advanced technology attachment (SATA) and the peripheral component expansion interface (PCIe) as public protocols. Where external non-volatile storage is supported, the administrator is to be able to close it and it is to be off by default; an external non-volatile memory used for identity authentication is not to hold user data other than the authentication information.

6.1.8 Configuration security. A function for maintaining the security configuration is to be provided, with query and modification carried out by the administrator; a self-test function is to be provided that demonstrates the correct operation of all or part of the security functions; where an operation panel exists, panel locking is to be supported.

6.2 Security assurance requirements

6.2.1 Design and development. The provider is to identify the security risks of the design and development stages, set a security policy and take measures protecting the design and development of the key components; establish and apply a secure development process that reduces the risk of malicious code being planted and of vulnerabilities being introduced; place design and development documents under configuration management with a configuration list and authorised, controlled change; carry out security testing of the device, including the third-party software and hardware modules it uses, on its own, jointly or through a third party; repair security defects and vulnerabilities found during development and operate an emergency repair process for those not found at that stage; ensure consistency between the design and the implementation of the security functions; and possess the capability to design and develop key components such as the driver, the firmware and the data control board.

6.2.2 Production and delivery. The provider is to describe all user-related function modules and access interfaces, including but not limited to man-machine and debug interfaces; declare, through the user agreement, the user manual or a website notice, that no