



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 38558-2020

**Information security technology - Security test method for
office devices**

Issued on: March 6, 2020

Implemented on: October 1, 2020

Issued by: SAMR; SAC

Table of Contents

Foreword	3
1 Scope	4
2 Normative references	4
3 Terms and definitions	4
4 Abbreviations	4
5 Test methods	5
5.1 Test of security technical requirements	5
5.2 Test of security management function requirements	8
Appendix A (Informative) Correspondence between the security test methods of this standard and the security requirements of GB/T 29244-2012	10

1 Scope

This standard specifies the test methods for security technical requirements and security management function requirements for office devices.

This standard applies to testing institutions and office device manufacturers to test the security of office device.

Note: The test method specified in this standard is applicable to the conformance test of GB/T 29244-2012. For the corresponding correspondence, see Appendix A.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 29244-2012 Information security technology - Basic security requirements for office devices

3 Terms and definitions

The terms and definitions defined in GB/T 29244-2012 apply to this document.

4 Abbreviations

The following abbreviations apply to this document.

I2C: Inter-Integrated Circuit SPI: Serial Peripheral Interface

5.1.3 Security audit

This test includes:

a) Check the product documentation of the office device to confirm whether the audit records include the following audit events:

- 1) Turn on and off the audit function;
- 2) Operation start and completion;
- 3) Use of identity authentication mechanism;
- 4) Use of identification mechanism;
- 5) Use of management functions;
- 6) Time change;
- 7) Other events related to system security or specifically defined auditable events.

Meanwhile test whether the audit records accurately record the corresponding audit events.

b) Check the audit records of office device, to see if the audit records include the date and time of the event, the type of event, the identity of the subject, the result of the event (success or failure), the type of task, and so on.

c) Test whether the office device has audited important security events such as user login, audit function on/off, user permission modification, time change; verify whether the audit event record is associated with the identity of the user who caused the event.

d) Check whether the office device has time management function and whether it provides reliable time stamp; whether it can prevent the audit record time from being tampered.

5.1.4 Protection of residual information

This test includes:

a) Check the residual information protection capabilities of office device;

verify whether the storage space of user data is completely destroyed before the data is released or redistributed to other users, or whether protective measures have been taken to make the residual information unusable;

5.1.8 Removable non-volatile storage

This test includes:

- a) Check whether the data storage of the removable non-volatile storage device has taken security measures, to protect user data, security function data, etc.;
- b) Check the data structure of the mobile non-volatile storage device, including whether the storage address, storage content, storage space length, etc. are public;
- c) Test whether the mobile non-volatile storage device exchanges data with the host of the office device through public interface protocols, such as SPI, I2C, etc.;
- d) Check whether the product documentation clearly identifies the storage capacity of the mobile non-volatile storage device;
- e) Test whether the removable non-volatile storage device in the office device can perform integrity check on the stored data (user data and security function data).

5.1.9 Password requirements

Check the product documentation provided by the office device supplier, to confirm whether the use and management of cryptographic technology complies with the relevant regulations of national cryptographic management.

5.2.1 Security attribute management

This test includes:

- a) Check whether the product documentation indicates that the office device has the function of initializing security attributes; reset the office device and check whether the office device is restored to the default value of the security attributes;
- b) Test whether office device restricts ordinary users from initializing security attributes;
- c) Test whether office device allows administrators or authorized users to perform maintenance operations on the user's security attributes;
- d) Check whether office device restricts ordinary users from operating