ICS 35.030
CCS L80

# 中华人民共和国国家标准

GB/T XXXXX—XXXX
代替 GB/T 30278—2013
代替 GB/T 35283—2017

# 信息安全技术
# 政务计算机终端核心配置规范

Information security technology—
Chinese government desktop core configuration specifications

（草案）

本稿完成时间：2023.05

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

## 1 范围

本文件规定了政务计算机终端核心配置对象、配置范围、配置要求、基线配置描述文件的格式规范、配置的自动化实现方法、实施流程，描述了配置要求对应的证实方法。

本文件参考网络安全等级保护基本要求的第三级要求提出核心配置基线制作规范，对于等级保护二级、四级要求，可适当裁剪、降低或增加、增强配置基线内容。

本文件适用于政务部门开展计算机终端的核心配置工作。

## 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件。不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 25100—2010 信息与文献 都柏林核心元数据元素集

GB/T 25647—2010 电子政务术语

GB/T 37950—2019 信息安全技术 桌面云安全技术要求

GB/T 40692—2021 政务信息系统定义和规范

ISO/IEC 18180:2013 信息技术 可扩展配置清单描述格式规范1.2版 （Information technology — Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2）

## 3 术语和定义

GB/T 22239—2019、GB/T 25069和GB/T 40692—2021界定的以及下列术语和定义适用于本文件。

3.1

**政务部门** government department

中共中央、全国人大、国务院、全国政协、国家监察委员会、最高人民法院、最高人民检察院及中央和国家机关各部门，各级地方党委、人大、政府、政协、监察委、法院、检察院及其直属各部门，以及法律法规授权具有行政职能的事业单位和社会组织。

[来源：GB/T 40692—2021，3.1]

3.2

**电子政务网** electronic government network

由基于电子政务传输骨干网的政务内网和政务外网组成的网络。

[来源：GB/T 25647—2010，3.1.6，有修改]

3.3

**政务计算机终端** government client computer

政务部门的桌面计算机、膝上型计算机和虚拟桌面等。

3.4

**虚拟桌面** virtual desktop

一种基于虚拟化技术所提供的桌面应用。

[来源：GB/T 37950—2019,3.2，有修改]

3.5

**核心配置项（配置项）** core configuration item

BIOS、计算机操作系统、办公软件、浏览器、电子邮件客户端、安全防护软件、即时通信软件等基础软件中影响计算机安全的关键参数配置项。

注：核心配置项类型包括开关项、枚举项、区间项和复合项，可以根据安全要求对其进行赋值。

3.6

**核心配置** core configuration

对核心配置项进行参数设置的过程。

注：通过核心配置限制或禁止存在安全隐患或漏洞的功能，启用或加强安全保护功能，来增强计算机抵抗安全风险的能力。

3.7

**核心配置项基值** core configuration item base value

按照核心配置基本要求对配置项的参数设置。

3.8

**核心配置基线** core configuration baseline

能够满足计算机安全基本要求的一组核心配置项基值构成的集合。

3.9

**核心配置要求清单** core configuration requirement list

由核心配置要求列项构成的一种列表，是对核心配置项属性的一种形式描述。

3.10

**核心配置基线包** core configuration baseline package

为实现核心配置基线自动化部署而制定的一种具有特定语法格式的核心配置数据文件。

3.11

**可信根** root of trust

始终以预期方式运行的单元。是系统的可信基点，也是实施安全控制的基点。

3.12

**可信验证** trusted verification

依据防护策略和基准值对防护对象进行主动度量和对度量结果判定的过程。

## 4 缩略语

下列缩略语适用于本文件。

BIOS：基本输入输出系统（Basic Input Output System）

CGDCC：政务计算机终端核心配置（Chinese Government Desktop Core Configuration）

GUID：全球唯一标识符（Globally Unique Identifier）

TCM：可信密码模块（Trusted Cryptography Module）

XCCDF：可扩展配置检查表描述格式（Extensible Configuration Checklist　Description Format）

XML：可扩展标记语言（Extensible Markup Language）

## 5　概述

### 5.1　核心配置对象

本标准针对应用于政务部门的联网计算机终端提出核心配置要求，包括连接到互联网、政务专网（政务内网、政务外网）的桌面计算机、膝上型计算机和虚拟桌面等。

### 5.2　核心配置范围

核心配置的范围包括如下方面：

a)　BIOS 软件；

b)　操作系统；

c)　办公软件（主要包括文档软件、表格软件、演示软件等）；

d)　浏览器软件；

e)　电子邮件客户端；

f)　安全防护软件（保护计算机运行安全的杀毒软件、审计软件和防火墙软件等）；

g)　即时通信软件。

依据GB/T 22239—2019中8.1.4和8.3.3对于第三级安全计算环境的要求，对上述基础软件的配置要求将从表1的安全要素提出。

表 1　安全要素表

| 安全要素 | 描述 |
|---|---|
| 身份鉴别 | 包括账户登录和凭证管理 |
| 访问控制 | 包括账户管理和权限分配 |
| 安全审计 | 包括账户行为审计和资源访问审计 |
| 入侵防范 | 包括对组件的保护功能开启、应用程序的更新升级 |
| 恶意代码防范 | 包括杀毒软件的安装、升级和病毒查杀管理 |
| 可信验证 | 包括可信验证配置和应用程序白名单管理 |
| 数据完整性 | 包括对终端上数据的完整性保存、传输的配置 |
| 数据保密性 | 包括对终端上数据的保密性保存、传输的配置 |
| 数据备份恢复 | 包括本地数据备份、异地实时备份和热冗余配置 |
| 剩余信息保护 | 包括临时文件、历史文件和虚拟文件管理 |
| 个人信息保护 | 包括对个人信息的收集、使用和展示的配置 |
| 应用管控 | 包括对应用安全性的配置和应用申请权限的配置 |

### 5.3　核心配置项赋值方法

a)　手动赋值

政务终端规模较小时，可参照本标准附录 D 编制核心配置要求清单，根据清单对核心配置项进行人工逐项赋值。例如，在 Windows 系统环境下，启动组策略编辑器，由人工对核心配置项进行赋值；在 Linux 系统环境下，手动编辑配置文件，对核心配置项逐项进行赋值；在 BIOS 中，直接在人机界面上，逐项进行手动赋值。

b) 自动赋值

对于有一定规模的政务终端，应根据附录 B 搭建自动化部署及监测体系，根据附录 A 将核心配置要求清单落实为核心配置基线包，根据附录 C 实施流程完成政务终端的自动化配置工作。附录 D 给出了将核心配置要求落实为核心配置要求清单的示例，附录 E 给出了将核心配置要求清单落实为基线配置文件的示例。

# 6 核心配置基本要求

## 6.1 BIOS 核心配置要求

### 6.1.1 身份鉴别

身份鉴别配置要求包括：

a) 应启动身份鉴别机制,并设置符合安全策略的 BIOS 口令长度、复杂度；
b) 应限制连续登录失败次数，达到登录失败次数后中止启动。

### 6.1.2 访问控制

访问控制配置要求包括：

a) 应限制使用定时开机、远程模式控制开机等开机模式；
b) 在启用管理员账户和普通用户账户时，管理员账户应配置启动顺序，并设置优先从本地磁盘启动，普通用户仅能查看启动顺序。

### 6.1.3 可信验证

可信验证配置要求包括：

a) 应默认开启可信根模块和可信验证功能；
b) 应启用对 BIOS 自身的可信验证功能。

### 6.1.4 数据保密性

数据保密性配置要求包括：

a) 在硬件支持的条件下，应配置硬盘访问口令；
b) 在硬件支持的条件下，应启用硬盘加密功能。

## 6.2 操作系统核心配置要求

### 6.2.1 身份鉴别

身份鉴别配置要求包括：

a) 账户登录时，应启动身份验证机制，限制连续登录失败次数，连续多次登录失败后应锁定账户；
b) 应配置远程网络认证策略，选择安全的身份认证协议、密码保护技术，如具有防重放、防暴力破解等机制；

c) 应启用账户鉴别数据存储安全配置，保护账户鉴别数据的存储安全和登录过程中的身份数据安全；
d) 使用基于口令鉴别登录用户身份时，应配置符合安全策略的口令长度、复杂度、有效期和加密强度，应提示用户修改默认口令、禁止不设置口令；
e) 使用基于数字证书技术鉴别登录用户身份时，应配置仅支持使用基于硬件的证书载体；
f) 可配置通过生物特征识别等安全技术作为身份鉴别依据，包括但不限于：指纹、人脸、声纹、虹膜、指静脉等生物特征识别。

注：附录D给出了身份鉴别配置要求清单示例。

#### 6.2.2 访问控制

访问控制配置要求包括：
a) 应禁用非必须账户、及时删除过期账户 ，给必须账户分配必要的最小权限集，例如禁用匿名账户（Anonymous）、来宾账户（Guest）、产品支持账户（Support），限用管理员账户（Administrator、root），限制普通用户的访问权限；
b) 应根据账户权限范围限制对文件、硬件、驱动、内存和进程等重要资源的访问权限；
c) 应限制非管理员账户权限提升操作；
d) 应限制开启对互联网提供服务接口，限制使用互联网远程协助服务。

#### 6.2.3 安全审计

安全审计配置要求包括：
a) 应启用账户安全日志，记录账户的创建、更改、删除、启用、禁用和重命名等操作，记录账户登录和注销、凭据验证、权限分配及变更、账户配置变更等操作；
b) 应启用系统日志，记录开关机信息，关键系统组件、程序的可信验证结果，对系统资源的访问及操作异常信息等。

#### 6.2.4 入侵防范

入侵防范配置要求包括：
a) 应禁止介质自动运行；
b) 应启用对系统组件数据的自我保护功能，例如：数据执行保护（DEP）模式；
c) 应启用登录账户超时锁定功能，并设置唤醒口令；
d) 应关闭不必要的服务和端口；
e) 应配置最小安装原则，仅安装必要的系统组件和程序；
f) 应保持操作系统安全补丁及时更新。

#### 6.2.5 可信验证

可信验证配置要求包括：
a) 操作系统安装后第一次初始化时，应启用并初始化可信根设备；
b) 每次启动、重启、休眠唤醒应启用对系统重要组件、配置参数等进行静态/动态的可信验证；
c) 系统应屏蔽特定的指令，避免可信根设备和设备内的数据被不恰当的设置、重置和读写，被非平台角色获取平台权限；
d) 系统应开启可信根的抗字典攻击保护功能。

#### 6.2.6 数据保密性

操作系统应开启基于密码技术的数据保护功能，保证政务终端上数据的保密性。

#### 6.2.7 数据备份恢复

应启用操作系统数据和用户数据的备份与恢复功能。

#### 6.2.8 剩余信息保护

剩余信息保护配置要求包括：

a) 应禁止剪贴板存储信息与远程计算机共享；
b) 关闭系统时，应清除虚拟内存页面文件；
c) 断开会话时，应清除临时文件夹；
d) 系统应配置定期清理临时文件。

#### 6.2.9 个人信息保护

个人信息保护配置要求包括：

a) 应配置禁止未授权访问和使用个人信息；
b) 应配置仅采集和存储必需的个人信息；
c) 应限制个人信息的使用权限。

#### 6.2.10 应用管控

应用管控配置要求包括：

a) 应只允许通过安全认证的应用软件安装和运行，例如经过数字签名的软件；
b) 应限制应用软件的访问权限，禁止未授权应用软件访问终端信息，修改终端资源配置，收集、修改、传输或删除终端数据。

#### 6.2.11 数据发送控制

数据发送控制配置要求包括：

a) 对于本地计算机个人及用户信息数据，应禁止发送到境外区域；
b) 对于系统运行数据（业务数据、日志数据、遥测数据等），应禁止发送到境外区域。

### 6.3 办公软件核心配置要求

办公软件核心配置要求包括：

a) 应禁止加载未签名插件；
b) 应禁止将用户数据发送到境外；
c) 应限用未数字签名的宏、脚本程序；
d) 应限制网上下载联机图片和模板等资源，限制访问超链接；
e) 应限制在线自动更新升级，保持办公软件安全补丁及时更新。

### 6.4 浏览器核心配置要求

#### 6.4.1 访问控制

访问控制配置要求包括：

a) 应默认开启浏览器的沙箱模式或安全模式；

b) 应默认开启浏览器内网页访问麦克风、摄像头、地址位置等设备的提示，并经过用户允许后才可以访问；
c) 应默认阻止加载未签名、不安全的第三方软件，例如：控件、插件、扩展程序；
d) 应默认开启追踪保护等隐私保护功能。

#### 6.4.2 入侵防范

入侵防范配置要求包括：
a) 若浏览器具备自我保护功能，应默认开启自我保护，防止非法软件侵害浏览器的运行安全；
b) 应开启下载安全扫描，默认阻止不安全的下载和执行；
c) 应保持浏览器软件安全补丁及时更新。

#### 6.4.3 个人信息保护

个人信息保护配置要求包括：
a) 应关闭浏览器输入框自动关联功能；
b) 应设置浏览器在用户知情同意前提下最小限度收集个人信息。

#### 6.4.4 剩余信息保护

应配置关闭网页时自动删除 Cookie 文件、下载记录、访问网站历史记录和临时文件，并清除其他缓存内容。

#### 6.4.5 数据发送控制

应关闭系统或软件内组件发送数据（用户数据、业务数据、日志数据、遥测数据等）到境外的功能。

### 6.5 电子邮件客户端核心配置要求

电子邮件客户端核心配置要求包括：
a) 应禁止直接运行附件中存在安全隐患的文件类型；
b) 应禁止直接打开邮件中的超链接；
c) 对本地存储的邮件数据应开启加密功能；
d) 应配置邮件的数字签名验签和加解密功能；
e) 应开启加密传输协议收发邮件；
f) 应启用垃圾邮件过滤功能；
g) 应配置在删除登录的邮箱账户后清理该账户缓存数据。

### 6.6 安全防护软件核心配置要求

安全防护软件核心配置要求包括：
a) 应启用安全审计功能，对每个用户行为和安全事件进行审计；
b) 应启用对审计记录的保护功能；
c) 应默认开启自我保护功能，防止自身被恶意破坏；
d) 应开启对终端计算机的实时保护功能；
e) 应设置及时升级安全防护软件，开启自动更新特征库等功能；
f) 应设置定期进行安全扫描功能，发现恶意文件等立即隔离并提醒用户执行后续操作；
g) 若 IT 环境允许、安全防护软件支持，可开启云查杀功能。

## 6.7 即时通信软件核心配置要求

### 6.7.1 身份鉴别

身份鉴别配置要求如下：

a) 应默认开启多次身份鉴别失败后的账户锁定功能；
b) 应默认开启口令安全性控制策略，包括口令长度、字符组成等，避免使用含有账号信息的口令及常见口令；
c) 应默认开启定期更改口令的策略。

### 6.7.2 访问控制

访问控制配置要求如下：

a) 应默认禁止普通用户执行发布群公告、设置群禁言、设置入群验证、解散群聊等重要行为的权限；
b) 应默认开启访问第三方业务资源的权限控制策略。

### 6.7.3 数据完整性和保密性

数据完整性和保密性配置要求如下：

a) 应默认开启数据传输过程中的数据加密能力；
b) 应禁止以明文形式将口令存储在系统中；
c) 若软件具有安全水印功能时，应默认开启该功能，显示位置宜包括：“聊天会话”、“通讯录”等，显示内容宜包括、“身份标识码”“姓名”、“日期”等；
d) 应默认开启本地磁盘中缓存数据加密的配置。

# 7 证实方法

## 7.1 BIOS 核心配置要求证实方法

### 7.1.1 身份鉴别

a) 测试方法：
   1) 检查 BIOS 身份鉴别机制是否启用，尝试设置不满足 BIOS 口令长度、复杂度要求的口令；
   2) 检查连续登录失败次数超过设定阈值时是否中止启动。
b) 预测结果：
   1) BIOS 身份鉴别机制已启用，尝试设置不满足 BIOS 口令长度、复杂度要求的口令失败；
   2) 连续登录失败次数超过设定阈值时 BIOS 中止启动。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.1.2 访问控制

a) 测试方法：
   1) 检查定时开机、远程模式控制开机等开机模式是否默认关闭；
   2) 在启用管理员账户和普通用户账户时，检查管理员账户是否配置启动顺序，并设置优先从本地磁盘启动，检查普通用户是否仅能查看启动顺序。
b) 预测结果：
   1) 定时开机、远程模式控制开机等开机模式已限制使用；

2） 管理员账户已配置启动顺序，并设置优先从本地磁盘启动，普通用户仅能查看启动顺序。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.1.3 可信验证

a） 测试方法：

1） 检查是否默认开启可信根模块和可信验证功能；

2） 检查 BIOS 自身的可信验证功能是否启用。

b） 预测结果：

1） 已默认启用可信根模块，开启可信验证功能；

2） 已启用 BIOS 自身的可信验证功能。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.1.4 数据保密性

a） 测试方法：

1） 在硬件支持的条件下，检查是否配置硬盘访问口令；

2） 在硬件支持的条件下，检查是否启用硬盘加密功能。

b） 预测结果：

1） 在硬件支持的条件下，已配置硬盘访问口令；

2） 在硬件支持的条件下，已启用硬盘加密功能。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2 操作系统核心配置要求证实方法

#### 7.2.1 身份鉴别

a） 测试方法：

1） 检查账户身份验证机制是否启用、是否配置登录失败重试次数，尝试连续登录失败超过设定阈值时是否锁定账户；

2） 检查远程网络认证策略项是否启用并选择了安全身份认证协议、密码保护技术，采用网络数据包分析等技术，验证是否经过安全身份认证协议、密码保护技术保护来往数据；

3） 检查账户鉴别数据存储相关的安全配置是否启用，是否可以通过本地、网络渠道另存为、修改等技术手段获取、修改用户鉴别数据和用户身份数据；

4） 检查系统口令长度、复杂度、有效期、加密强度的配置项是否启用并合理设置，当有默认口令时，是否提示用户修改默认口令，尝试不设置口令时是否提示设置失败；

5） 预配置系统使用基于数字证书技术鉴别登录用户身份时，尝试使用非基于硬件载体的证书登录系统，查看能否登录成功；

6） 当计算机终端有用于身份鉴别的生物特征识别设备时，检查生物特征识别设备是否默认启用。

b） 预测结果：

1） 账户身份验证机制启用，连续登录失败超过设定阈值时账户锁定；

2） 远程网络认证策略项已启用并选择了安全身份认证协议、密码保护技术，网络数据包分析结果为来往数据包受安全身份认证协议、密码技术保护；

3） 账户鉴别数据存储相关的安全配置已启用，通过本地、网络渠道的另存为、修改等技术手段无法获取、修改用户鉴别数据和用户身份数据；

4) 已启用系统口令长度、复杂度、有效期、加密强度的配置并设置适当值，当用户使用默认口令登录时提示用户修改默认口令，用户尝试清空或不设置口令时系统给出适当的禁止提示；
5) 系统已设置仅支持基于硬件的证书，尝试使用非基于硬件的数字证书（例如可以安装在计算机上的 pfx 格式的身份证书）时无法登录操作系统；
6) 当计算机终端有用于身份鉴别的生物特征识别设备时，设备已默认启用。

c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.2 访问控制

a) 测试方法：
1) 检查系统账户配置，是否存在非必须账户（例如：匿名账户（Anonymous）、来宾账户（Guest）、产品支持账户（Support））和过期多余账户；检查默认登录账户是否为管理员账户，检查系统所有账户权限配置，是否存在与其身份不符的访问权限；
2) 检查系统现有账户对系统资源的权限配置，如：文件、硬件、驱动、内存、进程等，是否存在与其身份不符的访问权限；
3) 检查非管理员账户是否可以进行未授权的账户权限提升操作；
4) 检查系统是否默认关闭对互联网提供服务的接口，是否默认关闭互联网远程协助服务。

b) 预测结果：
1) 系统中只存在必要账户，无过期账户；管理员账户非默认登录账户，所有账户权限与其身份相符，未分配超出角色范围的访问权限；
2) 系统现有账户对系统资源的权限配置与其身份相符，未分配超出其角色范围的访问权限；
3) 非管理员账户不可以进行非授权的账户权限提升操作；
4) 系统默认关闭了对互联网提供服务的接口，默认关闭了互联网远程协助服务。

c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.3 安全审计

a) 测试方法：
1) 检查账户安全日志是否启用，检查账户安全日志里是否记录了以下的各项操作：账户的创建、更改、删除、启用、禁用、重命名、账户登录和注销、凭据验证等；
2) 检查系统日志是否启用，检查系统日志是否记录了以下的各项信息：系统登录和注销信息、关键系统组件、程序的可信验证结果和对系统资源的访问及操作异常信息等。

b) 预测结果：
1) 账户安全日志启用，且记录了账户安全日志中的各项操作；
2) 系统日志启用，且记录了系统日志中的各项信息。

c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.4 入侵防范

a) 测试方法：
1) 将可以自动运行的介质插入系统，查看介质中的程序是否自动运行；
2) 检查系统组件数据的自我保护功能是否启用；
3) 检测系统是否适当设置账户超时锁定时间；检查超时后是否锁定屏幕；唤醒时，是否需要输入唤醒口令；
4) 使用系统自带或第三方工具检查操作系统是否开启了不必要的服务和端口；

5） 检测系统中是否安装有不必要的系统组件和程序；
6） 检查最新的安全补丁是否更新。

b） 预测结果：
1） 介质内程序未自动运行；
2） 已启用对系统组件数据的自我保护功能；
3） 系统超出空闲设定时间后，能锁定当前用户；系统被唤醒时，要求输入唤醒口令；
4） 系统仅开启了必要的服务和端口；
5） 系统满足配置最小安装原则，仅安装有必要的系统组件和程序；
6） 最新的安全补丁已更新。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.5 可信验证

a） 测试方法：
1） 操作系统初始化后，登录操作系统，查看可信根设备是否完成初始化；
2） 使用操作系统工具或第三方工具获取可信根的动态/静态验证结果；
3） 执行平台权限指令（例如：TCM2_PP_Commands），查看指令执行结果；
4） 在可信根中创建加密对象后，使用不同错误的口令重复尝试打开加密对象。

b） 预测结果：
1） 登录操作系统查看，系统显示当前终端计算机上可信根设备已就绪；
2） 根据工具获取的可信验证结果判定系统是否启用动态/静态验证，若无其他故障干扰时，无可信验证结果判定为未启用；
3） 平台权限命令执行失败；
4） 在超过尝试次数上限后，执行命令返回“对象已锁定”等近似表述的结果。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.6 数据保密性

a） 测试方法：
检查是否启用数据保护功能。

b） 预测结果：
数据保护功能启用。

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.7 数据备份恢复

a） 测试方法：
检查操作系统数据和用户数据的备份与恢复功能配置项是否配置、启用；执行数据备份、恢复操作，确认是否能将操作系统数据和用户数据成功备份，是否能将操作系统和用户备份的数据重新恢复。

b） 预测结果：
操作系统数据和用户数据备份与恢复功能配置项已配置启用；执行数据备份操作，操作系统数据和用户数据能成功备份；执行恢复操作，能成功恢复操作系统数据和用户备份数据；

c） 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.2.8 剩余信息保护

a) 测试方法：
   1) 在系统运行期间，检查是否可以通过远程计算机访问并获取剪切板存储信息；
   2) 系统关闭后，检查计算机存储中是否保留有虚拟内存页面文件；
   3) 系统会话断开后，检查系统临时文件夹区域中是否留有相应信息；
   4) 检查系统配置中是否设置了定期清理临时文件夹，并且在设定时间过后，检查系统临时文件夹是否被清理。
b) 预测结果：
   1) 在系统运行期间，用户无法通过远程计算机访问并获取剪切板存储信息；
   2) 系统关闭后，计算机存储中的虚拟内存页面文件已经被删除；
   3) 系统会话断开后，系统临时文件夹被清空；
   4) 系统启用了定期清理临时文件夹功能，并设置了间隔时间，在设定时间过后，系统临时文件夹被清理。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.2.9 个人信息保护

a) 测试方法：
   1) 检查是否配置禁止未授权访问和使用个人信息；
   2) 检查是否配置仅采集和存储必需的个人信息；
   3) 检查是否限制个人信息的使用权限。
b) 预测结果：
   1) 已配置禁止未授权访问和使用个人信息；
   2) 已配置仅采集和存储必需的个人信息；
   3) 已限制个人信息的使用权限。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.2.10 应用管控

a) 测试方法：
   1) 检查未通过安全认证的软件是否可以安装和运行；
   2) 检查应用软件的访问权限，非授权应用软件对指定数据读、写、删除行为结果。
b) 预测结果：
   1) 未通过安全认证的软件不可以安装和运行；
   2) 应用访问位置、摄像头等设备时提示用户选择是否允许，未授权软件无法对指定数据读、写、删除。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.2.11 数据外发控制

a) 测试方法：
   1) 采用网络数据包分析等技术手段检查系统是否将个人及用户信息数据发送到境外区域；
   2) 采用网络数据包分析等技术手段检查系统是否将运行中非必须的数据（业务数据、日志数据、遥测数据等）发送到境外区域。
b) 预测结果：
   1) 未发现个人及用户信息数据被系统送到境外区域；
   2) 未发现系统运行中非必须的数据被发送到境外区域。

c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

## 7.3 办公软件核心配置要求证实方法

a) 测试方法：
   1) 尝试加载未签名插件；
   2) 采用网络数据包分析等技术手段检查软件是否将用户数据发送到境外；
   3) 检查是否限用无数字签名的宏、脚本程序，并尝试运行未签名的宏、脚本程序；
   4) 尝试在软件内下载联机图片和模板等资源，尝试访问超链接行为；
   5) 检查是否默认关闭在线自动更新升级功能，检查最新的安全补丁是否更新。
b) 预测结果：
   1) 尝试加载未签名插件失败；
   2) 采用网络数据包分析等技术手段未发现软件将用户数据发送到境外的行为；
   3) 已配置限用无数字签名的宏、脚本程序，尝试运行未签名的宏、脚本程序失败；
   4) 软件内下载联机图片和模板等资源失败，超链接访问失败；
   5) 已配置默认关闭在线自动更新升级，最新安全补丁已更新。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

## 7.4 浏览器核心配置要求证实方法

### 7.4.1 访问控制

a) 测试方法：
   1) 启动浏览器，查看是否处于沙箱模式或安全模式；
   2) 检查浏览器内网页访问麦克风、摄像头、地址位置信息等是否有提示，用户允许/拒绝后网页反馈信息；
   3) 尝试为浏览器加载未签名、不安全的第三方软件，检查浏览器是否进行阻止；
   4) 访问收集个人浏览数据行为的网站，检查浏览器是否有禁止收集并提醒。
b) 预测结果：
   1) 启动浏览器后，默认进入沙箱模式或安全模式；
   2) 浏览器提示用户是否允许访问，用户允许后可以访问，否则拒绝访问；
   3) 浏览器阻止加载未签名、不安全的第三方软件；
   4) 浏览器阻止网站收集个人浏览数据行为。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.4.2 入侵防范

a) 测试方法：
   1) 若浏览器具备自我保护功能，使用第三方工具对正在运行的浏览器进行安全侵害（内存数据、代码修改等），检查浏览器是否可以正常运行；
   2) 使用浏览器下载文件，检查是否进行安全扫描，并阻止不安全的文件下载和运行；
   3) 检查浏览器软件安全补丁版本与官网最新版本是否一致。
b) 预测结果：
   1) 若浏览器具备自我保护功能，浏览器开启自我保护，可以防止非法软件侵害浏览器的运行；
   2) 浏览器下载文件可以进行安全扫描，成功阻止不安全的文件下载和运行；
   3) 浏览器软件安全补丁与官网浏览器版本一致。

c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.4.3 个人信息保护

a) 测试方法：
   1) 启动浏览器地址栏中输入网址并有提交操作，关闭浏览器，再次启动浏览器并访问该网址，检查是否能够自动关联该网址；
   2) 检查浏览器安装时是否有用户服务协议、隐私政策等提示信息，并查看完整的服务协议和隐私政策。
b) 预测结果：
   1) 浏览器地址栏未自动关联之前的已访问网址；
   2) 安装浏览器时提示用户服务协议、隐私政策，并可以阅读完整条款。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.4.4 剩余信息保护

a) 测试方法：
   关闭浏览器并重启浏览器，查看浏览器是否存在访问记录和下载文件的历史记录和临时文件。
b) 预测结果：
   浏览器无 Cookie 文件、下载记录、访问网站历史记录和临时文件。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

#### 7.4.5 数据外发控制

a) 测试方法：
   采用网络数据包分析等技术手段检查浏览器组件是否将数据（用户数据、业务数据、日志数据、遥测数据等）发送到境外区域。
b) 预测结果：
   采用网络数据包分析等技术手段未发现浏览器组件将数据发送到境外区域。
c) 结果判定：上述预期结果均满足判定为符合，其他情况判定为不符合。

### 7.5 电子邮件客户端核心配置要求证实方法

a) 测试方法：
   1) 尝试运行邮件中具有安全隐患的文件类型附件（例如可执行程序、脚本、宏）；
   2) 尝试打开邮件中的超链接；
   3) 使用文本分析等工具或技术，尝试打开本地存储的邮件数据文件；
   4) 检查是否开启邮件的数字签名验签，检查是否开启邮件加解密功能；
   5) 采用网络数据包分析等技术手段检查来往数据包是否采用加密传输协议；
   6) 检查电子邮件客户端是否启用并合理设置垃圾邮件过滤功能；
   7) 检查被删除账户是否存在内存和硬盘等缓存数据。
b) 预测结果：
   1) 运行邮件中具有安全隐患的文件类型附件失败；
   2) 打开邮件中的超链接失败；
   3) 使用文本分析等工具或技术，尝试打开本地存储的邮件数据文件，文件内容加密，不可读取；
   4) 邮件的数字签名验签、邮件加解密功能已开启；