ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32925—2016

信息安全技术　政府联网计算机终端安全管理基本要求

Information security technology—Basic security requirements for networked computer terminal of government

2016-08-29 发布　　2017-03-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由工业和信息化部提出。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)归口。

本标准起草单位:北京信息安全测评中心、国家计算机网络应急技术处理协调中心、中国科学院软件研究所、中国铁路总公司运输局信息化部、黑龙江省信息安全测评中心、北京市石景山区经济和信息化委员会、北京朋创天地科技有限公司、黄山市委市政府信息办公室、北京市统计局计算中心。

本标准主要起草人:刘海峰、钱秀槟、王春佳、赵章界、张晓梅、梁博、李晨旸、贺海、孙永生、舒敏、苏璞睿、刘刚、黄俊强、王燕春、李晓勇、曹卫东、王晓路、强倩、王希忠、宋超臣、卢跃庆、史蓉。

引　言

本标准是GB/T 29245—2012《信息安全技术　政府部门信息安全管理基本要求》框架下的政府部门信息安全保障标准体系的组成部分，用于指导各级政府部门对所管辖范围内联网计算机终端的管理和安全检查工作，使其具备一定的安全防护能力。本标准可与各种具体的计算机终端应用场景、操作系统和应用软件的配置指南配合使用。另外，政府部门可根据自身工作特点，按照“综合防护”“适度保护”的原则选择使用，在满足基本要求的基础上，选择执行附录A中的增强安全要求，以进一步提高本部门联网计算机终端的安全防护水平。

信息安全技术　政府联网计算机终端安全管理基本要求

1　范围

本标准规定了政府部门联网计算机终端的安全要求。

本标准适用于政府部门开展联网计算机终端安全配置、使用、维护与管理工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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—2008　信息安全技术　信息系统安全等级保护基本要求

GB/T 25069—2010　信息安全技术　术语

GB/T 29245—2012　信息安全技术　政府部门信息安全管理基本要求

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

计算机终端　computer terminal

供个人日常办公使用的、能独立进行数据处理及提供网络服务访问的台式微型计算机系统、便携微型计算机系统、瘦客户机系统或虚拟终端系统等，不包含智能移动终端(如掌上电脑、智能移动电话等)。

3.2

联网　networked

联接政府部门非涉密办公局域网。

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)

CPU：中央处理器(Central Processing Unit)

IP：网络之间互连的协议(Internet Protocol)

MAC：介质访问控制(Media Access Control)

USB：通用串行总线(Universal Serial Bus)

5　计算机终端安全总体要求

5.1　安全策略制定

联网计算机终端的安全策略应是本单位总体信息安全策略的重要组成部分，并为单位的信息安全

总体目标服务。安全策略的制定应从人员管理、资产管理、软件管理、接入安全、运行安全、BIOS 配置要求等方面综合考虑。

5.2 安全防护要求

处理或保存敏感程度较低数据的联网计算机终端，如处理一般性公文或访问无敏感信息的政务系统等的联网计算机终端，安全防护应满足本标准正文所提出的安全基本要求；保存或处理较敏感信息的联网计算机终端，如处理敏感公文、访问有敏感信息的政务系统、发布门户网站信息的联网计算机终端，或 GB/T 22239—2008 规定的三级以上信息系统中的计算机终端，在满足本标准正文要求的基础上，还应满足附录 A 所规定的增强要求。

5.3 文件管理要求

应将与联网计算机终端安全管理和支撑日常维护工作的各类软硬件使用相关的规范、流程、操作指导书等制定成文件(文件需考虑要素可参见附录 B)。文件应通过正式有效的方式发布，并确保计算机终端管理和使用人员能够获取、理解和执行。

6 人员管理要求

6.1 角色和责任

6.1.1 应按照 GB/T 29245—2012 中第 3 章的要求，明确信息安全主管领导、指定信息安全管理机构、配备专职或兼职信息安全员，将计算机终端的信息安全管理纳入职责范围，建立健全计算机终端信息安全管理的责任制和工作机制。

6.1.2 应按照 GB/T 29245—2012 中 4.3 要求，指定专职或兼职资产管理人员，负责计算机终端相关资产的管理。

6.1.3 承担计算机终端安全管理工作的专职或兼职信息安全员，应由政府部门在编或长期聘用人员担任，且接受过培训(见 6.2.3)并经过考核。信息安全员应满足互备要求。

6.2 岗位管理与培训

6.2.1 应按照 GB/T 29245—2012 中 4.2a)的要求，建立健全岗位信息安全责任制度，明确信息安全员和计算机终端使用人员在计算机终端方面的信息安全责任；信息安全员和计算机终端使用人员应签订信息安全与保密协议，明确信息安全与保密责任。

6.2.2 应按照 GB/T 29245—2012 中 4.2b)的要求，制定并执行人员离岗离职信息安全管理规定。人员离职应终止或调整该人员使用的计算机终端访问各种资源的权限、清理或隔离该计算机终端上存储的数据信息，并应在签署的信息安全保密承诺书中涵盖计算机终端相关保密要求。

6.2.3 应按照 GB/T 29245—2012 中第 7 章的要求，加强对信息安全员和计算机终端使用人员的信息安全教育培训，提高信息安全意识，掌握信息安全防护基本技能。培训内容包括但不限于信息化相关法律法规、信息安全意识、信息化和信息安全常识和基础技能、计算机软件安装、计算机软件安全配置及安全使用等；培训频次应不低于每年一次。应对信息安全员定期考核。

6.2.4 政府部门长期聘用人员在计算机终端安全管理方面的要求应等同于政府部门本单位人员。

6.3 临时访问人员管理

6.3.1 临时访问人员要访问政府部门内部信息系统，应使用政府部门专用的计算机终端设备。应对临时人员的访问行为进行监控和审计。

6.3.2 临时访问人员自带的计算机终端接入办公局域网要履行审批手续，批复中要明确允许接入的子

网，并对接入子网的人员加强管理。

7 资产管理要求

7.1 采购

7.1.1 应按照 GB/T 29245—2012 中 4.4 的要求，采购安全可控的计算机终端及其配套的软硬件产品。

7.1.2 应选择安全可控的安全防护类软件，如恶意代码防范软件、本机防火墙等。

7.1.3 采购计算机终端运维服务，应满足 GB/T 29245—2012 中 4.5 的要求。

7.1.4 定制开发的软件安装到联网计算机终端之前，应由信息安全管理机构组织源代码安全审查。

7.2 登记与使用维护

7.2.1 资产管理人员应按照 GB/T 29245—2012 中 4.3 的要求建立并维护计算机终端软硬件资产清单，并根据资产清单定期进行盘点。硬件资产清单中应包含硬件设备的名称、编号、品牌型号、采购时间、领用人或存放位置、领用时间等信息；软件资产清单应包含软件名称、版本号、采购时间、开发方名称、用途或使用人等信息。

7.2.2 计算机终端因维修或其他原因带离办公区域时，应根据所存储数据的安全属性，由终端使用人员采取数据备份、数据清除等措施，并履行登记手续，确保重要数据安全。在重新接入办公局域网前，应由信息安全员进行安全性检查。

7.2.3 资产管理人员应按照 GB/T 29245—2012 中 5.7 的要求对移动存储介质进行集中统一管理，并记录介质领用、交回、维修、报废、销毁等情况。移动存储介质使用人员应定期清理移动存储介质，避免长期保存数据信息。

7.2.4 发生计算机终端或移动存储介质数据丢失或损坏时，应由信息安全员或信息安全管理机构进行数据恢复；需要送外部做数据恢复时，应经信息安全主管领导书面同意，并选择可信的数据恢复专业机构。

7.3 报废与停用

7.3.1 应按照 GB/T 29245—2012 中 4.3 的要求，对计算机终端、移动存储介质等资产的报废统一管理，报废前应做好数据备份和清除，必要时可拆除硬盘、存储卡等数据存储介质。保存敏感信息的废弃存储介质，应由政府部门指定的有资质的机构进行回收处理。

7.3.2 软件授权使用时限到期、失去使用价值报废等情况下，应办理停用，并从计算机终端中卸载。

8 软件管理要求

8.1 软件安装

8.1.1 应根据计算机终端支撑业务开展的需求，建立并维护计算机终端软件选用列表。软件选用列表可包含系统软件、应用软件和安全防护软件等类别。其中系统软件包括操作系统、系统补丁等；应用软件包括网页浏览软件、邮件客户端软件、文档编辑软件、输入法软件、文件阅读软件、图片查看软件、媒体播放软件等，还可包括财务软件、远程管理软件和专用业务系统客户端等；安全防护软件包括恶意代码防护软件、本机防火墙等。

8.1.2 应按照各计算机终端的实际需求，从计算机终端软件选用列表中选择安装操作系统、应用软件及相关组件、安全防护软件等，并由信息安全管理机构负责统一安装。

8.1.3 应规定应用软件的安装目录和数据存储目录，数据存储目录应独立于系统分区。

8.2 操作系统配置管理

8.2.1 应使用非系统管理员账号作为日常办公的账号，不应使用其他高权限或特殊权限账号进行日常办公操作，不应将日常办公用的普通账号赋予系统管理员权限、其他高权限或特殊权限。应删除或禁用系统中的特殊账号、临时账号。

8.2.2 应设置操作系统账号口令保护机制，不应使用空口令登录系统；口令应由字母、数字及特殊字符组成，长度不小于8位；应设置账户锁定阈值，并设置登录失败次数超过阈值后的安全策略；应设置口令更新周期，口令更新周期不应超过3个月。

8.2.3 应设置并启用带口令的屏幕保护程序，设定屏幕保护等待时间。

8.2.4 应关闭默认共享，确需共享的应按照最小权限原则明确共享文件夹的共享权限。

8.2.5 应关闭对移动存储介质的自动播放功能。

8.2.6 应关闭不必要的端口和服务。

8.2.7 应限制远程管理服务。如确有需要开启远程管理服务，应对远程接入的账号、地址范围等进行限制。

8.2.8 应设置时钟同步，统一联网计算机终端的时钟。

8.2.9 应为网络连接设置统一、可信的域名解析服务器IP地址，并至少设置1个备用的域名解析服务器IP地址。

8.3 应用软件配置管理

8.3.1 网页浏览器

对网页浏览器的要求包括：

a) 应设置统一、可信的初始页面或将初始页设置为空白页；
b) 应根据需要建立网页浏览器插件或组件列表，不应随意安装网页浏览器插件和组件；
c) 应禁用网页浏览器自动加载应用程序的功能；
d) 应设置下载文件的统一存储目录，存储目录应为数据存储目录中的独立子目录；
e) 应设定本地缓存空间大小，并定期清理本地缓存、Cookie、历史记录以及临时文件内容。

8.3.2 邮件客户端软件系统

对邮件客户端软件系统的要求包括：

a) 针对不同的邮箱账号，应设置易识别的账号标识信息。
b) 应按照GB/T 29245—2012中5.5的要求，设置邮箱账号访问口令。邮箱账号访问口令由字母、数字及特殊字符等组成，长度不小于8位。邮箱账号访问口令应不同于操作系统口令，并定期更新，更新周期不应超过3个月。
c) 应建立独立于邮件客户端软件安装目录之外的邮件保存目录，邮件保存目录应为数据存储目录中的独立子目录。
d) 应禁用或限制邮件客户端软件系统对带格式邮件、附件的自动处理或显示功能。
e) 应定期清理保存在邮件服务器上的邮件信息，定期清除、转移或归档计算机终端上的邮件。

8.3.3 文档编辑软件

对文档编辑软件的要求包括：

a) 应设置用于标识用户的基本信息；
b) 应限制文档编辑软件自动批量处理功能；

c) 应通过软件自身功能或通过本机防火墙限制文档编辑软件访问外部网络；
d) 应启用文档定时保存功能。

8.4 安全防护软件配置管理

8.4.1 恶意代码防范软件设置为开机自动启动方式。
8.4.2 设置对本机数据进行定期安全扫描。
8.4.3 设置对浏览器、邮件客户端软件、即时通讯软件等方式下载的资源进行安全扫描。
8.4.4 设置对接入介质进行自动安全扫描。
8.4.5 启用软件及特征库的自动更新功能。
8.4.6 应启用本机防火墙，并以白名单的方式设置访问控制规则。

9 接入安全要求

9.1 网络接入

9.1.1 应建立计算机终端接入网络的审批制度。
9.1.2 应根据各内设部门的工作职能和处理业务的重要程度，划分不同的子网，并制定各子网间的访问规则和策略。
9.1.3 应制定对计算机终端在网络上的统一命名规则，名称应易于识别。
9.1.4 应设置并启用网络接入控制策略，通过实名接入认证、限制物理接入点、IP 地址与 MAC 地址绑定等措施，将接入的计算机终端限定在指定的物理子网或逻辑子网中。
9.1.5 应将临时访问人员自带的计算机终端，接入经过批准的子网中，并在接入网络前对其采取病毒木马检测和清除措施。
9.1.6 应限制计算机终端通过无线方式接入办公局域网。如确有需要通过无线方式接入，应采取权限限制、设置接入口令、使用安全协议等手段加强保护。
9.1.7 应限制远程接入的计算机终端数量、接入方式、访问范围等。

9.2 介质接入

9.2.1 应对介质接入实行统一管理，进行接入控制并记录介质使用情况。
9.2.2 按照 GB/T 29245—2012 中 5.7 的要求，介质接入计算机终端前，应查杀病毒、木马等恶意代码。

10 运行安全要求

10.1 统一管理

10.1.1 应制定计算机终端软件安装和变更审批制度，对软件安装和变更进行统一管理。因工作需要增加、减少安装软件或对软件进行升级及其他配置变更前，应按照审批流程进行审核；审核批准并备案后，由责任部门或责任人对相关计算机实施软件变更或监督实施软件变更，同时更新软件配置清单。
10.1.2 应按照 GB/T 29245—2012 中 5.6 的要求，采用集中统一管理方式对联网计算机终端进行管理，统一软件下发、漏洞扫描、补丁安装、病毒库升级和病毒查杀等。

10.2 监控审计

10.2.1 操作系统审计

本项要求包括：

a) 应设置操作系统日志审计，对账号登录、策略更改、对象访问、服务访问、系统事件、账户管理等行为进行日志记录。日志记录的内容应包括事件发生的时间、主体、客体、行为(结果)等。
b) 安全防护软件应启用日志审计，对攻击事件拦截、病毒查杀等行为进行记录。日志记录的内容应包括时间、事件类别、事件描述、操作处理等。
c) 应设置审计日志保留时间不少于7天，并设置审计日志文件大小、文件达到设定值或无存储空间时的操作方式。
d) 应由信息安全员定期对计算机终端的审计日志进行审查。

10.2.2 流量监控

应监测网络带宽使用情况，并能对指定计算机终端的带宽使用进行限制。

10.2.3 软件漏洞扫描

应对计算机终端进行定期安全漏洞扫描，并通过正规渠道获取操作系统及应用软件的补丁程序。

10.3 备份管理

10.3.1 应定期备份重要数据。
10.3.2 本机备份时应保存在不同的磁盘分区。
10.3.3 介质备份时应使用专用的存储介质。
10.3.4 需要异地备份时，应由专人管理维护。
10.3.5 应定期检查备份数据的可用性、完整性。

10.4 信息安全事件管理

10.4.1 应按照GB/T 29245—2012中第6章的要求，建立健全信息安全应急工作机制。
10.4.2 应建立计算机终端发生数据丢失、木马病毒感染等安全事件报告和事件响应机制，并制定文件描述报告和响应的流程、职责和处置权限。
10.4.3 应保留信息安全事件发生状况、所采取的措施和处理结果等的记录。
10.4.4 应按照GB/T 29245—2012中4.2d)的要求对信息安全责任事故进行查处。

10.5 监督检查

10.5.1 信息安全管理机构应按照GB/T 29245—2012中第7章的要求，每年至少对计算机终端进行一次定期的信息安全检查，并向计算机终端使用者通报信息安全检查结果。
10.5.2 信息安全管理机构应根据安全检查结果，完善相关的安全管理制度和技术防护措施，提高计算机终端的安全防护能力。

10.6 例外处置

10.6.1 当联网计算机终端暂时不能满足部分安全要求，可以申请例外处置，经信息安全主管领导批准后进行例外处置并备案。
10.6.2 例外处置申请应至少包含计算机终端编号、型号、配置、使用人、申请例外处置的原因、不能满足的要求、临时处理方法、例外处置期限、整改措施、整改期限、整改责任人等。
10.6.3 信息安全员应对例外处置及整改情况进行监督，并向信息安全主管领导汇报。

附 录 A
（规范性附录）
政府联网计算机终端安全增强要求

A.1 BIOS 配置要求

要求包括：

a） 开机时应启动身份鉴别机制，并设置安全的口令长度和复杂度；

b） 应限制硬件资源使用，包括软驱、硬盘、内存、USB 设备、网卡和 CPU 等；

c） 应启用硬盘写保护；

d） 应限制由外部设备，如 U 盘、光驱、软驱等引导驱动计算机终端。

A.2 软件管理要求

A.2.1 操作系统

本项要求包括：

a） 终端为多人共用时，应为不同的人员设立不同的账户，并根据最小权限原则分配权限；

b） 操作系统的账号口令应包含大写字母、小写字母、数字、特殊字符等四类字符，且账号口令应与其他的鉴别方式（如动态口令、数字证书等）配合使用；

c） 操作系统补丁程序在安装前应进行测试。

A.2.2 应用软件

A.2.2.1 一般要求

本项要求包括：

a） 应以软件选用列表为基础，建立计算机终端可执行程序“白名单”，通过终端管理系统、安全防护软件等技术手段阻止非“白名单”软件的安装和运行；

b） 应用软件补丁程序在安装前应进行测试；

c） 应定期检查计算机终端软件正版化的情况，卸载非授权使用软件。

A.2.2.2 网页浏览器

要求包括：

a） 应禁用网页浏览器缓存功能；

b） 应禁用网页浏览器自动保存用户名和密码等表单信息功能。

A.2.2.3 邮件客户端软件系统

应配置连接邮件服务器的方式，确保数据加密传输。

A.2.2.4 文档编辑软件

要求包括：

a） 应禁用文档编辑软件的网络功能；

b） 应限制文档编辑软件在本地保存副本或临时文件；
c） 应对重要文档应设置口令保护，限制对文档的读写；
d） 应开启文档编辑软件的安全功能，不运行不明的插件和编程功能。

A.2.3 安全防护软件

应安装统一的恶意代码防范软件。

A.3 接入安全要求

A.3.1 网络接入

要求包括：
a） 应对接入办公局域网的计算机终端进行认证，通过认证后方可使用网络资源；
b） 应对办公局域网内计算机终端的外联进行限制；
c） 应能够对内部网络用户未经准许联到外部网络的行为进行检查。

A.3.2 介质接入

要求包括：
a） 接入联网计算机终端的移动存储介质应支持加密功能；
b） 应能检查接入的移动存储介质的合法性；
c） 应限制使用联网计算机终端的 USB 接口为手机等外部设备充电。

A.4 运行安全要求

A.4.1 监控审计

要求包括：
a） 应依照联网计算机终端软件运行需求，启用并配置软件进程监测策略，对违反策略的行为进行处置；
b） 应依照联网计算机终端软件选用列表，启用并配置软件审计策略，对软件的增加、修改、删除等变更操作进行审计；
c） 应通过集中监控审计系统对联网计算机终端网络行为进行安全监控和审计，审计日志数据保存时间应不低于 60 天；
d） 应能对移动存储介质接入联网计算机终端的行为进行审计。

A.4.2 趋势跟踪

应进行联网计算机终端的安全趋势跟踪，以便及时发现安全风险并进行处置。

附 录 B
（资料性附录）
政府联网计算机终端安全管理制度要素

政府部门在制定文件化的联网计算机终端安全管理制度时，可包含如下要素，这些要素可以包含在机构的整体安全制度体系中，也可针对联网计算机终端单独制定，可以是一个制度文件，也可以由多个制度文件分别规范：

a） 联网计算机终端安全基本策略（是机构安全策略的一部分）；
b） 计算机终端安全管理的职责和工作机制；
c） 岗位信息安全责任，明确信息安全员和计算机终端使用人员的信息安全与保密责任；
d） 信息安全培训要求；
e） 人员离岗离职信息安全管理规定、长期外协或外聘人员管理规定、临时访问人员管理；
f） 计算机终端软件安装审批制度、计算机终端软件列表；
g） 计算机终端的运维、监控、审计、备份等要求；
h） 计算机终端的安装和使用规程；内容可包含：操作系统配置操作规程、系统重装和恢复指导书、应用软件配置指导书等；
i） 计算机终端相关资产的管理要求。内容可包含：计算机终端及相关设备维修时的数据保护要求、存储介质处理要求、移动存储介质使用登记备案要求，计算机终端相关资产清单等；
j） 信息安全事件时的报告和响应流程、职责和处置权限；
k） 定期对联网计算机终端进行安全检查和通报的要求；
l） 计算机终端例外处置程序。