ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37095—2018

信息安全技术　办公信息系统安全基本技术要求

Information security technology—Security basic technical requirements for office information systems

2018-12-28 发布　　2019-07-01 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

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准主要起草单位:中国电子技术标准化研究院、工业和信息化部软件与集成电路促进中心、深圳赛西信息技术有限公司、工业和信息化部电子第五研究所、北京赛西科技发展有限公司、中国交通通信信息中心、西安电子科技大学、北京工业大学。

本标准主要起草人:范科峰、姚相振、刘贤刚、高林、杨建军、戴明、唐一鸿、毕思文、叶润国、许东阳、龚洁中、孙康健、刘龙庚、刘帅、王莉、李云婷、裴庆祺、杨震。

信息安全技术　办公信息系统安全基本技术要求

1　范围

本标准规定了办公信息系统的安全基本技术要求。

本标准适用于指导党政部门的办公信息系统建设，包括在系统设计、产品采购、系统集成等方面应遵循的基本原则，以及应满足的基本技术要求。涉密办公信息系统的建设管理依据相关国家保密法规和标准要求实施。

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 2887—2011　计算机场地通用规范

GB/T 18018　信息安全技术　路由器安全技术要求

GB 18030—2005　信息技术　中文编码字符集

GB/T 20272　信息安全技术　操作系统安全技术要求

GB/T 20273　信息安全技术　数据库管理系统安全技术要求

GB/T 20275—2013　信息安全技术　网络入侵检测系统技术要求和测试评价方法

GB/T 20281—2015　信息安全技术　防火墙技术要求和测试评价方法

GB/T 21028—2007　信息安全技术　服务器安全技术要求

GB/T 21050—2007　信息安全技术　网络交换机安全技术要求(评估保证级 3)

GB/T 21052—2007　信息安全技术　信息系统物理安全技术要求

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 26856—2011　中文办公软件基础要求及符合性测试规范

GB/T 28452—2012　信息安全技术　应用软件系统通用安全技术要求

GB/T 29240—2012　信息安全技术　终端计算机通用安全技术要求与测试评价方法

GB/T 33190—2016　电子文件存储与交换格式　版式文档

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

办公信息系统　office information system

由服务器、桌面 PC、操作系统、数据库管理系统、应用服务器中间件、办公软件、网络设施、应用软件系统等软硬件组成，通过数据的收集、存储、传递、管理和处理等手段，提供办公服务的信息系统。

3.2

用户相关信息　user related information

使用办公信息系统的自然人或法人的信息及其元数据。

注：用户相关信息包括用户个人信息，办公信息系统中用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据等。

3.3

第三方测试机构　third party test organization

与产品供应方、产品应用方等相关各方均独立的专业测试机构。

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）

CA：认证授权（Certificate Authority）

CPU：中央处理器（Central Processing Unit）

PC：个人计算机（Personal Computer）

USB：通用串行总线（Universal Serial Bus）

5　基本原则

5.1　标准符合原则

办公信息系统所采用的软硬件产品在功能性、性能、可靠性、安全性等方面应符合相关的国家标准。

5.2　开放兼容原则

办公信息系统所采用的软硬件产品应在同类产品之间可替换，并支持两种或以上操作系统架构，相关产品之间应具备良好的兼容适配性，保证办公信息系统的互操作性和可移植性。

5.3　安全性原则

办公信息系统软硬件产品提供商应当为其产品、服务持续提供安全维护；不得在产品中预置、加载禁用安全机制或绕过安全机制的功能；承诺在产品维护升级更新活动中，不侵害用户信息安全；收集用户个人敏感信息前，应取得用户的明示同意；不将搜集掌握的用户相关信息在境外存储和处理，不得泄露和非法使用；在规定或者当事人约定的期限内，不得终止提供安全维护。

5.4　功能最小化原则

办公信息系统所采用的软硬件产品的功能应满足办公实际需求，相关产品应支持从功能上进行裁剪，避免与办公应用无关的冗余功能。

5.5　透明可验证原则

办公信息系统所采用的软硬件产品宜接受国家认定的第三方测试机构的检测和验证，以证明其与相关标准的符合性；厂商应为检测验证提供其产品的相关接口、协议、加密方式等；第三方测试机构在检测和验证过程中，应维护企业知识产权、商业秘密和用户信息，不得将企业提供的技术细节用于检测和验证以外的目的。

6 技术要求

6.1 概述

本章对办公信息系统部署和运维的物理环境提出了要求，并对办公信息系统的重要组成部分，包括基础软硬件产品、网络设施、应用软件系统提出了要求。

6.2 通用要求

办公信息系统应按照 GB/T 22239—2008 的第三级及以上要求进行设计、建设和运维。

6.3 物理环境

办公信息系统的物理环境应满足以下要求：

a) 办公信息系统部署、运维的机房建设应符合 GB/T 2887—2011 的相应要求；

b) 办公信息系统部署、运维的物理环境应符合 GB/T 21052—2007 的相应要求。

6.4 基础软硬件产品

6.4.1 硬件产品

6.4.1.1 服务器

6.4.1.1.1 服务器硬件指标

服务器硬件指标应符合 GB/T 21028—2007 中第三级及以上安全要求。

6.4.1.1.2 BIOS

服务器的 BIOS 要求主要包括：

a) BIOS 的配置界面应支持中文显示；

b) BIOS 应支持固件软件安全升级；

c) 针对 CPU 及芯片组固件驱动、操作系统内核等，BIOS 应支持上述设备经过国家认可的第三方 CA 机构颁发的代码签名验证。

6.4.1.2 桌面 PC

6.4.1.2.1 桌面 PC 硬件指标

桌面 PC 硬件指标主要包括：

a) 应符合 GB/T 29240—2012 中安全技术要求第三级及以上要求；

b) 应提供禁止无线网络模块、红外模块、蓝牙模块、接入 USB 设备的功能。

6.4.1.2.2 BIOS

桌面 PC 的 BIOS 要求主要包括：

a) BIOS 的配置界面应支持中文显示；

b) BIOS 应支持固件软件安全升级；

c) 针对 CPU 及芯片组固件驱动、操作系统内核等，BIOS 应支持上述设备经过国家认可的第三方 CA 机构颁发的代码签名验证。

6.4.2 软件产品

6.4.2.1 操作系统

操作系统的技术要求主要包括：

a) 字符编码应符合 GB 18030—2005 的规定；
b) 操作系统及操作系统相关的安全部件应符合 GB/T 20272 中的三级及以上要求；
c) 应拥有灵活的访问控制策略，提供文件系统完整性检查工具，监视重要的文件和目录发生的改变；
d) 应提供操作系统防火墙配置工具；
e) 应支持口令、数字证书等多种身份认证机制；
f) 应支持底层 BIOS 对操作系统的安全验证及启动；
g) 不应自行安装不带有有效证书签名的软件和固件组件；
h) 应建立策略来管理软件的安装，防止未授权软件安装；
i) 应强制执行最低限度密码复杂度，保障账户安全；
j) 应在操作系统中安装防篡改保护程序，保护系统组件和系统服务；
k) 应支持进程级独立的安全审计功能，能够记录所有成功和不成功的操作；
l) 应支持保护系统残留信息安全；
m) 不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件；
n) 操作系统厂商应为产品测试提供所供应产品的接口、协议、加密方式等；
o) 操作系统厂商应支持按用户的需求对所供应产品的功能进行裁剪。

6.4.2.2 数据库管理系统

数据库管理系统的技术要求主要包括：

a) 字符编码应符合 GB 18030—2005 的规定；
b) 应符合 GB/T 20273 的规定；
c) 数据库管理系统厂商应为与其他厂商数据库之间的数据迁移提供支持；
d) 不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件；
e) 数据库管理系统厂商应为产品测试提供所供应产品的接口、协议、加密方式等；
f) 数据库管理系统厂商应支持根据用户需求对所供应产品的功能进行裁剪。

6.4.2.3 应用服务器中间件

应用服务器中间件的技术要求主要包括：

a) 字符编码应符合 GB 18030—2005 的规定；
b) 应支持对应用的部署、调试和卸载，应提供对系统性能进行监控和调优、日志管理的管理工具，宜提供支持 Web 组件开发的可视化集成开发工具；
c) 应支持保证数据源恢复和保证事务一致性的系统故障恢复能力；
d) 应支持对进出的网络数据流进行实时监控；
e) 应支持对登录用户进行身份标识和鉴别；
f) 应支持访问控制功能，控制用户对服务器数据的访问；
g) 不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件；
h) 应用服务器中间件厂商应为产品测试提供所供应产品的接口、协议、加密方式等；
i) 应用服务器中间件厂商应支持按用户需求对所供应产品的功能进行裁剪。

6.4.2.4 应用软件

应用软件的技术要求主要包括：

a) 字符编码应符合 GB 18030—2005 的规定；
b) 应符合 GB/T 26856—2011 的规定；
c) 版式文档应符合 GB/T 33190—2016 的规定；
d) 应提供支持多种浏览器的插件；
e) 应提供对文件进行加密的选项；
f) 不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件；
g) 应用软件厂商应为产品测试提供所供应产品的接口、协议、加密方式等；
h) 应用软件厂商应支持根据用户需求对所供应产品的功能进行裁剪。

6.5 网络设施

6.5.1 主要网络设备

6.5.1.1 交换机

交换机应符合 GB/T 21050—2007 的规定。

6.5.1.2 路由器

路由器应符合 GB/T 18018 中第三级安全要求的规定。

6.5.2 主要安全设备

6.5.2.1 防火墙

防火墙应符合 GB/T 20281—2015 的规定。

6.5.2.2 入侵检测系统

入侵检测系统应符合 GB/T 20275—2013 中技术要求部分的规定。

6.6 应用软件系统

6.6.1 功能性

应用软件系统应坚持功能最小化原则，基本功能要求如下：

a) 系统应支持公文管理功能
   ——应支持公文流转功能，可包含拟稿、核稿、编辑、审核、撤销、退回、签发、选择下一环节、发送、签收、会签、登记、拟办、审阅、分办、承办、办结、归档等；
   ——应支持增加和删除附件功能；
   ——应支持流程跟踪和查看功能；
   ——应支持添加正文功能；
   ——应支持保存公文草稿、查询公文、删除公文功能；
   ——应支持催办设置功能。
b) 系统应支持归档管理功能
   ——应支持公文归档功能；
   ——应支持归档查询功能。

c） 系统应支持公告功能

——应支持公告的新建、修改、删除、发布功能。

d） 系统应支持通知功能

——应支持通知的新建、修改、删除、发布功能。

e） 系统应支持会议管理功能

——应支持会议室管理功能，包括新建、修改、删除、查询会议室；

——应支持会议安排功能，包括新建、修改、删除、查询、打印会议信息。

f） 系统应支持个人工作区功能

——应支持个人待办、个人已办功能。

g） 系统应支持个人信息管理功能

——应支持修改个人信息功能；

——应支持修改个人密码功能。

h） 系统应支持在线人员列表功能

——应支持在线人员的姓名、所属部门、职位信息等。

i） 系统应支持后台管理员用户，管理员支持用户管理、统一权限管理等功能

——应支持用户的新建、修改、删除功能；

——应支持基于功能授权功能；

——应支持基于用户授权功能。

6.6.2 安全性

应用软件系统安全性技术要求如下：

a） 应符合 GB/T 28452—2012 中应用软件系统安全技术要求第三级及以上要求；

b） 不应存在隐蔽接口，不应加载能够禁用安全机制或绕过安全机制的组件；

c） 应在用户明示同意后，方可收集用户相关信息，并在收集用户相关信息时显示提示信息；

d） 在应用软件系统维护升级更新活动中，不得侵害用户信息安全。

6.6.3 可靠性

应用软件系统可靠性技术要求如下：

a） 系统应支持 7×24 h 的稳定无故障运行；

b） 系统应支持数据有效性检验功能，保证输入的数据格式或长度符合系统设定的要求；

c） 对于用户“非法”的输入或操作，系统不崩溃、不退出；

d） 系统应支持自动保护功能，当故障发生时能自动保护当前所有状态，保证系统能够进行恢复。

6.6.4 易用性

应用软件系统易用性技术要求如下：

a） 系统应提供用户使用手册，且手册中的功能描述与软件的实际功能一致；

b） 系统研制过程中形成的所有文档，语言简练、前后一致、易于理解以及语句无歧义；

c） 系统页面布局要合理，不宜过于密集或过于空旷，合理利用空间；

d） 系统的提示、警告或错误说明应该清楚、明了、恰当，避免歧义；

e） 编辑页面中的必输项应给出标识；

f） 对于用户非法的输入或操作，系统应给予提示信息，且提示信息能引导用户进行正确输入或操作；

g） 对可能造成数据无法恢复的操作，系统应给予提示信息，给用户放弃选择的机会；

h) 日期类型数据输入应提供日历选择功能；

i) 系统应支持 Ctrl＋A 全选、Ctrl＋C 拷贝、Ctrl＋V 粘贴、Ctrl＋X 剪切、Ctrl＋Z 撤消等快捷操作；

j) 对于有多个输入框的页面，系统应支持通过 Tab 键变更光标焦点，按照从左到右、从上到下的原则。