ICS
点击此处添加中国标准文献分类号

中 华 人 民 共 和 国 国 家 标 准

GB/T XXXXX—XXXX

信息安全技术
办公信息系统安全可靠基本技术要求

Information security technology - Security and reliable technical basic requirements for office information systems

点击此处添加与国际标准一致性程度的标识

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX

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、软件与集成电路促进中心、工业和信息化部电子第五研究所、深圳赛西信息技术有限公司、北京赛西科技发展有限公司、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、唐一鸿、孙康健、刘龙庚、刘帅、李云婷、裴庆祺、杨震

办公信息系统安全可靠基本技术要求

1 范围

本标准规定了办公信息系统的安全可靠基本技术要求，产品选型应遵循的基本原则。

本标准适用于指导党政部门的办公信息系统建设，包括系统设计、产品采购、系统集成等。

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 18030-2005《信息交换用汉字编码字符集基本集的扩充》

GB/T 28821-2012《信息技术 关系数据管理系统技术要求》

GB/T 26856-2011《信息技术 中文办公软件基础要求及符合性测试规范》

GB/T 20916-2007《信息技术 中文办公软件文档格式规范》

GB/T 18019-1999《信息技术 包过滤防火墙安全技术要求》

GB/T 26269-2010《网络入侵检测系统技术要求》

GB/T 28454-2012《信息技术 安全技术 入侵检测系统的选择、部署和操作》

GB/T 21052-2007《信息安全技术 信息系统物理安全技术要求》

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 21026-2007 《信息技术 中文办公软件应用编程接口规范》

GB/T 9704-2012《党政机关公文格式》

GB/T 21050-2007《信息安全技术 网络交换机安全技术要求》

GB/T 18018-2007《信息安全技术 路由器安全技术要求》

GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》

GB/T 20275-2006《信息安全技术 入侵检测系统技术要求和测试评价方法》

GB/T 20270-2006《信息安全技术 网络基础安全技术要求》

3 术语和定义

下列术语和定义适用于本文件。

3.1

信息系统 information system

信息系统由计算机及其相关的配套部件、设备和设施构成，按照一定的应用目的和规则对信息进行采集、加工、存储、传输、检索等的人机系统。

3.2

信息系统物理安全 physical security for information system

为了保证信息系统安全可靠运行，确保信息系统在对信息进行采集、处理、传输、存储过程中，不致受到人为或自然因素的危害，而使信息丢失、泄露或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境人员、系统等采取适当的安全措施。

3.3

服务器 server

服务器是信息系统的主要组成部分，是信息系统中为客户端计算机提供特定应用服务的计算机系统，包括标准机架式服务器、塔式服务器、刀片式服务器三种形态。

3.4

操作系统安全 security of operating system

操作系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.5

操作系统安全技术 security technology of operating system

实现各种类型的操作系统安全需要的所有安全技术。

3.6

数据库系统 database system

储存、管理、处理和维护数据的软件系统，主要由数据库、数据库管理系统和数据库管理员组成。

3.7

数据库管理系统 database management system

用于建立、使用和维护数据库的软件。

3.8

数据库管理系统安全 security of database management system

数据库管理系统所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.9

数据库管理系统安全技术 security technology of database management system

实现各种类型的数据库管理系统安全需要的所有安全技术。

3.10

中间件 middleware

为业务系统的运行提供运行支撑环境，提供系统运行必须的容器服务、名录服务、数据库连接池服务、邮件服务、安全服务等。

3.11

中间件安全 security of middleware

中间件所存储、传输和处理的信息的保密性、完整性和可用性的表征。

3.12

中间件安全技术 security technology of middleware

实现中间件安全需要的所有安全技术。

3.13

应用服务器 Application Server

web 应用服务器中间件

3.14

中文办公软件Chinese office software

用于中文办公处理的一套完整的计算机应用程序和相关文档，主要包括文字处理、电子表格和演示文稿3个应用软件。

3.15

路由器 router

路由器是主要的网络节点设备，工作在网络层，通过路由选择算法决定流经数据的存储转发，并具备访问控制和安全扩展功能。

3.16

防火墙 firewall

一个或一组在不同安全策略的网络或安全域之间实施访问控制的系统。

3.17

入侵检测系统 intrusion detection system

用于监测信息系统中可能存在的影响信息系统资产的行为的软件或软硬件组合。它通常分为主机型和网络型两种，由控制台、探测器和/或主机代理组成。

3.18

网络安全基础技术 basis technology of network security

实现各种类型的网络系统安全需要的所有基础性安全技术。

3.19

应用软件系统 application software system

信息系统的重要组成部分，是指信息系统中对特定业务进行处理的软件系统。

3.20

数据完整性 data integrity

数据完整性泛指数据库中数据的正确性和一致性，包括实体完整性、参照完整性和用户定义完整性。

4.符号和缩略语

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：数字证书认证中心（Certificate Authority）

CPU：中央处理器 （Central Processing Unit）

DHCP：动态主机设置协议（Dynamic Host Configuration Protocol）

FTP：文件传输协议（File Transfer Protocol）

IP：网际协议（Internet Protocol）

MPP：大规模并行处理系统（Massive Parallel Processing）

PC：个人计算机（Personal Computer）

PDF：便携文件格式（Portable Document Format）

SSL：安全套接层（Secure Sockets Layer）

TCP：传输控制协议（Transport Control Protocol）

4 产品选型基本原则

4.1 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。

4.2 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。

4.3 安全性原则

办公信息系统软硬件产品提供商不得在产品中预置、加载禁用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；不将搜集掌握的用户相关信息在境外存储和处理。

4.4 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。

4.5 透明可验证原则

办公信息系统所采用的软硬件产品应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。

5 技术要求

5.1 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 《计算机场地通用规范》相应的的要求；

b) 办公信息系统部署、运维的物理环境应符合 GB/T 21052-2007《信息安全技术 信息系统物理安全技术要求》的要求。

5.2 基础软硬件产品

5.2.1 硬件产品

5.2.1.1 服务器

服务器整机包括标准机架式服务器、塔式服务器、刀片式服务器三种形态。

5.2.1.1.1 服务器硬件指标

服务器硬件指标主要包括：

a) 内存：服务器的主板应支持内存扩展；

b) 网络接口性能：应支持 1000Mb/s 及以上的网络接入速度。

5.2.1.1.2 固件软件

服务器BIOS固件软件要求主要包括：

a) BIOS 支持系统硬件信息显示；

b) BIOS 的配置界面应支持中文显示；

c) BIOS 支持固件软件升级的能力；

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

5.2.1.2 桌面 PC

5.2.1.2.1 桌面 PC 硬件指标

桌面PC硬件指标主要包括：

a) 内存：办公用桌面 PC 内存应不低于 256MB；

b) 网络接口性能：应支持 100Mb/s 及以上的网络接入带宽；

c) 提供禁止无线网络模块、红外模块等的功能。

5.2.1.2.2 BIOS 固件软件

桌面PCBIOS固件软件要求如下：

a) BIOS 支持系统硬件信息显示；

b) BIOS 的配置界面应支持中文显示；

c) BIOS 支持固件软件升级的能力；

d) BIOS 支持对 CPU 驱动、操作系统内核等的经过国家认可的第三方 CA 机构颁发的代码签名验证。

5.2.2 软件产品

5.2.2.1 服务器操作系统

服务器操作系统的技术要求主要包括：

a) 应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》；
b) 应参照 GB/T 20272-2006《信息安全技术 操作系统安全技术要求》中的三级及以上要求；
c) 应提供支持设备驱动程序的添加和删除的管理工具；
d) 应提供系统故障监视与自动恢复、用于系统维护的系统信息采集等功能；
e) 应支持负载均衡集群，支持内核参数的配置；
f) 应支持 TCP/IP 等常用网络协议，应支持服务器常用应用软件包，包括 Web 服务器、域名服务器、DHCP 服务器、代理服务器、文件打印和共享服务器以及 FTP 服务器等软件包，并支持针对这些服务的本地及远程图形界面管理工具；
g) 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；
h) 应提供防火墙配置工具；
i) 应支持口令、数字证书等多种身份认证机制；
j) 应支持底层 BIOS 对操作系统的安全验证及启动；
k) 应禁止在操作系统中安装没有带证书签名的软件和固件组件；
l) 操作系统应建立策略来管理软件的安装，防止未授权软件安装；
m) 操作系统应强制执行最低限度密码复杂度，保障账户安全；
n) 应使用加密机制来保护存储在操作系统数字媒体控制区以外的运输过程中的信息的保密性和完整性；
o) 应支持对操作系统和其安装的应用进行漏洞扫描的能力，并标识和报告可能影响系统或应用的新漏洞；
p) 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；
q) 操作系统应支持在用户丢失密码密钥时维持信息的可用性的能力；
r) 应检测软件和信息的未授权变更并通过执行操作系统的完整性扫描重新评价软件和信息的完整性；
s) 应支持缓冲区溢出防护机制、rootkit 防护机制和内核密封技术等；
t) 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；
u) 应禁用客体重用机制，保护系统剩余信息安全；
v) 服务器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；
w) 服务器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。

5.2.2.2 桌面操作系统

桌面操作系统的技术要求主要包括：

a) 应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》；
b) 应参照 GB/T 20272-2006《信息安全技术 操作系统安全技术要求》中的三级及以上要求；
c) 应至少提供形码类、音码类等常用汉字输入法，宋体、仿宋、黑体、楷体、小标宋体等五种基本输出字体；
d) 应支持点阵、曲线两种中文字库，支持中文图形操作界面，并支持中文打印；
e) 应支持打印机、投影仪、扫描仪、数码相机等外围设备；
f) 应支持电子日历、计算器、文本编辑器、多媒体播放、图像处理等常用工具；
g) 应支持硬件配置、用户管理和桌面管理等工具；

h) 应支持 FTP、Telnet 等网络客户端应用；应支持邮件客户端、浏览器等上网工具；应支持实现跨操作系统的打印机等网络资源共享；
i) 应禁止在操作系统中安装没有带证书签名的软件和固件组件；
j) 操作系统应建立策略来管理软件的安装，防止未授权软件安装；
k) 操作系统应强制执行最低限度密码复杂度，保障账户安全；
l) 应使用加密机制来保护存储在操作系统数字媒体控制区以外的运输过程中的信息的保密性和完整性；
m) 应支持对系统和其安装的应用进行漏洞扫描的能力，并标识和报告可能影响系统或应用的新漏洞；
n) 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；
o) 操作系统应支持在用户丢失密码密钥时维持信息的可用性的能力；
p) 应检测软件和信息的未授权变更并通过执行操作系统的完整性扫描重新评价软件和信息的完整性；
q) 桌面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；
r) 桌面操作系统厂商应支持按用户需求对所供应产品的功能进行裁剪。

5.2.2.3 数据库管理系统

数据库管理系统的技术要求主要包括：

a) 应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》；
b) 应符合 GB/T 28821-2012《信息技术 关系数据管理系统技术要求》；
c) 应符合 GB/T 20273-2006《信息安全技术 数据库管理系统安全技术要求》中的三级及以上要求；
d) 应支持库级全量备份、库级增量备份、表级全量备份等备份功能；应支持库级全量还原、库级增量还原、表级全量还原等还原功能；应支持事务故障恢复功能；应支持库级的数据库复制、模式级的数据库复制、表级的数据库复制等功能；
e) 应支持数据库监控、死锁监测等性能监测与查询优化功能；
f) 应为与其他厂商数据库之间的数据迁移提供支持；
g) 应支持处理数据分析及多机并行查询功能；
h) 应支持行存表、列存表混合存储、检索技术；
i) 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；
j) 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。

5.2.2.4 应用服务器

应用服务器的技术要求主要包括：

a) 应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》；
b) 应支持事务服务、消息服务、安全服务、名字和目录服务、邮件服务、数据访问服务、企业应用集成服务等一系列基本服务；
c) 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；
d) 应支持在不中断系统运行的情况下动态部署和卸载应用的功能；
e) 应支持高速缓存、负载平衡、失效恢复的第三方 Web 服务器；应具有与其他应用系统连接和集成的能力；
f) 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；

g) 应用服务器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) 应用服务器厂商应具备根据用户需求对所供应产品的功能进行裁剪的能力；
i) 应在服务器网络接口部分对进出的网络数据流进行实时监控；
j) 应在应用服务器中设置防恶意代码软件，对所有进入服务器的恶意代码采取相应的防范措施，防止恶意代码侵袭；
k) 应采取措施保证服务器中数据的完整性和保密性；
l) 应用服务器应支持对登录用户进行身份标识和鉴别；
m) 应支持访问控制功能，控制用户对服务器数据的访问；
n) 应支持抵御拒绝服务攻击的能力，如，部署边界保护装置，增加容量、带宽并结合服务冗余；
o) 服务器应在通信会话结束时或在静默后终止与该会话相关联的网络连接；
p) 应用服务器应保护公共可用信息和应用的完整性和可用性；
q) 应用服务器应部署垃圾邮件防护机制，检测通过电子邮件，电子邮件附件、web 访问或者其他通用方法传送的非请求的消息，并采取相应措施；

5.2.2.5 办公软件

办公软件的技术要求主要包括：
a) 应符合 GB/T 26856-2011《信息技术 中文办公软件基础要求及符合性测试规范》；
b) 应符合 GB/T 20916《信息技术 中文办公软件文档格式规范》；
c) 应符合 GB 18030-2005《信息交换用汉字编码字符集基本集的扩充》；
d) 应符合 GB/T 21026-2007 《信息技术 中文办公软件应用编程接口规范》；
e) 应符合 GB/T 9704-2012《党政机关公文格式》中所规定的电子公文格式模板及排版；所规定的电子公文格式模板及排版应符合 GB/T 9704-2012《党政机关公文格式》；
f) 应提供支持多种浏览器的插件；
g) 应提供对文件进行加密的选项；
h) 应支持文件编辑过程中定时备份的功能；
i) 应支持 PDF 文件，具有 PDF 阅读工具，可打开查阅 PDF 文件，能导出成为 PDF 格式，并可以对导出的 PDF 格式文件进行打印、选择、加密等控制操作；
j) 办公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；
k) 办公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。

5.3 网络设施

5.3.1 主要网络设备

5.3.1.1 交换机

交换机安全性要求：
应符合 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。

5.3.1.2 路由器

路由器安全性要求：
应符合 GB/T 18018-2007《信息安全技术 路由器安全技术要求》。

5.3.2 主要安全设备

5.3.2.1 防火墙

防火墙的技术要求主要包括：

a) 应符合 GB/T 20281-2006《信息安全技术 防火墙技术要求和测试评价方法》。

5.3.2.2 入侵检测系统

入侵检测系统的技术要求主要包括：

应符合 GB/T 26269-2010《网络入侵检测系统技术要求》；

应符合 GB/T 28454-2012《信息技术 安全技术 入侵检测系统的选择、部署和操作》；

应符合 GB/T 20275-2006《信息安全技术 入侵检测系统技术要求和测试评价方法》。

5.4 应用系统

5.4.1 功能性

应用系统功能性技术要求主要包括：

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，正文应符合 GB/T 20916《信息技术 中文办公软件文档格式规范》的正文格式；

——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。

5.4.2 安全性

5.4.2.1 身份标识与鉴别

身份标识与鉴别应满足以下要求：

a) 系统应支持专用的登录控制模块对登录用户进行身份标识和鉴别；
b) 系统应支持用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；
c) 系统应支持登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；
d) 系统应支持单点登录的功能；

5.4.2.2 访问控制

访问控制应满足以下要求：

a) 系统应支持访问控制功能，控制用户对文件、数据库表等客体的访问；
b) 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；
c) 应由授权主体配置访问控制策略，并严格限制默认账户的访问权限；
d) 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
e) 应严格控制用户对有敏感标记重要信息的操作；
f) 系统应支持信息流控制功能，按适用策略系统内和互连系统之间的信息流进行控制；
g) 应对系统允许的远程访问方法形成文档，包括用途限制和实施指南等；
h) 应对系统未授权的远程访问进行监控；
i) 应使用相应的密码技术来保障系统远程访问会话的保密性和完整性；
j) 应禁止应用系统在没有使用规定的边界保护设备时直接与外网连接；

5.4.2.3 残余信息保护

残余信息保护应满足以下要求：

a) 残余信息能被有效清除；
b) 办公信息系统可能存在残余信息的资源类型及位置，应在产品文档资料中已明确告知。

5.4.2.4 安全审计

安全审计应满足以下要求：

a) 系统应支持覆盖所有用户的安全审计功能，对应用系统重要安全事件进行审计；
b) 应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；
c) 审计记录的内容至少应包括事件的日期、事件、发起者、类型、描述和结果等；
d) 系统应提供对审计记录进行统计、查询及生成审计报表的功能；
e) 应在系统安全审计处理失败时向管理员报警并采取相应的行动；
f) 应对安全审计信息和审计工具进行保护，避免未授权访问、修改和删除；
g) 应在系统建立内部连接前对系统组件进行安全合规性检查；

5.4.2.5 数据完整性

数据完整性应满足以下要求：

a) 应能够阻止非授权用户修改或破坏系统管理数据、鉴别信息和重要数据；
b) 应能够检测到系统管理数据、鉴别信息和重要数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；
c) 应能够检测到系统管理数据、鉴别信息和重要数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

5.4.2.6 密码技术

系统中所采用的密码技术，应满足国家密码主管部门的要求。

5.4.2.7 边界保护

边界防护应满足以下要求：
a) 应监视并控制发生在应用系统外部边界上和系统内的关键内部边界上的通信；
b) 应对应用系统连接外部网络或其它系统的接口上使用系统规定的边界保护装置；

5.4.3 可靠性

办公信息系统可靠性应满足以下技术要求：
a) 系统应支持 7×24 小时的稳定无故障运行；
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；
e) 系统应支持将操作系统和其他关键的系统软件的副本，以及系统的目录（包括硬件、软件和固件部件）的副本存放到与业务运行系统不在同一处的分隔开的设施或者防火的容器中；

5.4.4 易用性

办公信息系统易用性应满足以下技术要求：
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。