ICS 35.040
L 80

中华人民共和国国家标准

GB/T 37094—2018

信息安全技术
办公信息系统安全管理要求

Information security technology—Security management 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、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:姚相振、刘贤刚、范科峰、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
办公信息系统安全管理要求

1 范围

本标准规定了办公信息系统的建设管理、系统运维管理、制度管理和外包管理方面的要求。

本标准适用于指导党政部门的办公信息系统安全管理工作，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 25069—2010 信息安全技术 术语

GB/T 32926—2016 信息安全技术 政府部门信息技术服务外包信息安全管理规范

GB/T 37095—2018 信息安全技术 办公信息系统安全基本技术要求

GB/T 37096—2018 信息安全技术 办公信息系统安全测试规范

3 术语和定义

GB/T 25069—2010 和 GB/T 37095—2018 界定的术语和定义适用于本文件。

4 管理要求

4.1 建设管理

4.1.1 方案设计

方案设计要求如下：

a) 业主单位指定或授权专门的部门，根据办公信息系统建设原则和建设需求，编制建设的总体规划、技术框架和详细设计方案，制定建设工作计划和管理制度，并形成配套文件；

b) 应组织相关部门和专家对建设中采用的总体规划、技术框架、详细设计方案等相关配套文件的合理性和科学性进行论证，并且经过业主单位批准后，才能正式实施。

4.1.2 产品采购和使用

产品采购和使用要求如下：

a) 应根据办公信息系统建设原则和建设需求选择基础设施、设备、软硬件产品等，可预先对产品进行选型测试；

b) 产品选择应依据以下基本要求：

——应符合 GB/T 37095—2018 中针对各产品的技术要求；

——应依据 GB/T 37096—2018 由产品厂商、第三方测试机构、用户共同进行测试，并由第三方测试机构出具相应证明文件；

——相关产品厂商应承诺不私自收集用户信息；对掌握的用户信息进行有效保护，不在未授权情况下境外存储或处理掌握的用户信息；

——相关产品厂商应作出在售后服务中能够提供原厂服务的承诺。

c) 应确保密码产品采购和使用符合国家密码主管部门的要求；

d) 应指定或授权专门的部门负责产品的采购；

e) 产品使用时需遵守相关国家部门或单位规定。

4.1.3 软件开发

软件开发要求如下：

a) 应制定软件开发管理制度，明确软件设计、开发、测试、验收过程的控制方法和人员行为准则；

b) 应制定软件设计和开发的相关文档，包括软件设计文件、源代码、测试文档、使用手册和维护手册等；

c) 软件交付前应委托第三方测试机构依据开发要求的技术指标，对软件功能和性能等进行验收测试，并检测源代码中可能存在的恶意代码。

4.1.4 工程实施

工程实施要求如下：

a) 应选择具备计算机信息系统集成资质的信息系统集成商作为工程实施的承接单位；

b) 应制定详细的工程实施方案控制实施过程，实施方案包括工程时间限制、进度控制和质量控制等方面内容；

c) 应制定工程实施方面的管理制度，包括工程实施过程的控制方法、实施参与人员的行为准则等方面内容；

d) 应指定或授权专门的部门或人员负责工程实施过程的管理，可通过第三方工程监理控制项目的实施过程。

4.1.5 测试验收

测试验收要求如下：

a) 在测试验收前应根据设计方案或合同要求等制订测试验收方案；

b) 应委托第三方测试机构对系统进行验收测试，并出具验收测试报告；

c) 应组织相关部门和相关人员对系统测试验收报告进行评审；

d) 应组织相关专家、相关部门和相关人员召开项目验收会，并形成验收意见。

4.1.6 系统交付

系统交付要求如下：

a) 应制定系统交付清单，并根据交付清单对所交接的设备、软件和文档等进行清点；

b) 应对负责系统运行维护的技术人员进行相应的技能培训，形成培训记录，记录培训内容、培训时间和参与人员等；

c） 应确保提供系统建设过程中的文档和指导用户进行系统运行维护的文档。

4.1.7 服务商选择

服务商选择要求如下：

a） 应确保服务商的选择符合国家的有关规定；

b） 应与选定的服务商签订相关的协议，明确约定相关责任，协议内容包含服务内容、培训和服务承诺、保密范围、安全责任、违约责任、协议的有效期限等。

4.2 系统运维管理

4.2.1 环境管理

环境管理要求如下：

a） 应建立机房管理制度，内容覆盖机房物理访问、物品带进和带出机房、机房环境维护等；

b） 应指定专门的部门或人员定期对机房供配电、空调、温湿度控制等设施进行维护，形成维护记录，记录维护日期、维护人、维护设备、故障原因、维护结果等方面内容；

c） 应指定部门负责机房安全，对机房的出入、服务器的开机或关机等工作进行管理。

4.2.2 资产管理

资产管理要求如下：

a） 应编制并保存与信息系统相关的资产清单，包括资产责任部门、重要程度和所处位置等内容；

b） 应建立资产管理制度，规定信息系统资产管理的责任人员或责任部门，并规范资产管理和使用的行为。

4.2.3 设备管理

设备管理要求如下：

a） 应对信息系统中的基础软硬件产品、主要网络设备和主要安全设备等指定专门的部门或人员定期进行维护管理，形成设备维护记录；

b） 应建立基于申报、审批和专人负责的设备管理制度，对信息系统中的基础软硬件产品、主要网络设备和主要安全设备等的选型、采购、发放和领用等过程进行规范化管理；

c） 应确保基础软硬件产品、主要网络设备和主要安全设备经过审批才能带离机房或办公地点；

d） 应对信息系统中的移动存储设备建立严格的安全管理制度和流程，指定专门的安全人员负责移动存储设备的采购、使用和销毁等活动。

4.2.4 监控管理

监控管理要求如下：

a） 应对通信线路、主机、网络设备和应用软件的运行状况、网络流量等进行监测和报警，形成记录并妥善保存；

b） 应组织相关人员定期对监测和报警记录进行分析、评审，形成分析报告，并采取必要的应对措施。

4.2.5 安全管理

4.2.5.1 网络安全管理

网络安全管理要求如下：

a) 应指定专人对网络进行管理，负责运行日志、网络监控记录的日常维护和报警信息分析和处理工作；

b) 应建立网络安全管理制度，对网络安全配置、日志保存时间、安全策略、升级与打补丁、口令更新周期等方面作出规定；

c) 应根据厂家提供的软件升级版本对网络设备进行更新，并在更新前对现有的重要文件进行备份；

d) 应定期对网络系统进行漏洞扫描，对发现的网络系统安全漏洞进行及时的修补。

4.2.5.2 系统安全管理

系统安全管理要求如下：

a) 应根据业务需求和系统安全分析确定系统的访问控制策略；

b) 应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补；

c) 应安装系统的最新补丁程序，在安装系统补丁前，首先在测试环境中测试通过，并对重要文件进行备份后，方可实施系统补丁程序的安装；

d) 应建立系统安全管理制度，对系统安全策略、安全配置、日志管理和日常操作流程等方面作出具体规定；

e) 应定期对运行日志和审计数据进行分析，以便及时发现异常行为，异常行为包括账户的连续多次登录失败、非工作时间的登录、访问受限系统或文件的失败尝试、系统错误等。

4.2.5.3 恶意代码防范管理

恶意代码防范管理要求如下：

a) 应提高所有用户的防病毒意识，及时告知防病毒软件版本，在读取移动存储设备上的数据以及网络上接收文件或邮件之前，先进行病毒检查，对外来计算机或存储设备接入网络系统之前也应进行病毒检查；

b) 应指定专人对网络和主机进行恶意代码检测并保存检测记录；

c) 应提供恶意代码防范管理文档，内容是否覆盖防恶意代码软件的授权使用、恶意代码库升级、定期汇报等方面。

4.2.5.4 密码管理

密码技术和产品的使用应遵照国家密码管理规定。

4.2.6 变更管理

变更管理要求如下：

a) 应确认系统中要发生的变更，并制定变更方案，方案覆盖变更类型、变更原因、变更过程、变更前评估等方面的内容；

b) 系统发生变更前，向主管领导申请，变更和变更方案经过评审、审批后方可实施变更，并在实施

后将变更情况向相关人员通告；

c） 系统发生变更前应制定变更失败恢复程序，规定变更失败后的恢复流程。

4.2.7 备份与恢复管理

备份与恢复管理要求如下：

a） 应识别需要定期备份的重要业务信息、系统数据及软件系统等；

b） 应建立备份与恢复管理相关的管理制度，对备份信息的备份方式、备份频度、存储介质和保存期等进行规范；

c） 应根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略须指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法。

4.2.8 应急响应管理

应急响应管理要求如下：

a） 应在统一的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程、事后教育和培训等内容；

b） 应急预案需要定期审查和根据实际情况更新，形成审查和更新记录；

c） 应对系统相关的人员进行应急预案培训，形成培训记录；

d） 应急预案的培训应至少每年举办一次。

4.2.9 维修和报废管理

维修和报废管理要求如下：

a） 应指定或授权专门的部门或人员负责信息技术相关产品的维修和报废；

b） 应对信息技术相关产品的维修和报废管理指定规章制度；

c） 在信息技术相关产品维修和报废前，应确保存储有用户数据信息的磁介质或其他介质已经被卸除。

4.3 制度管理

4.3.1 管理制度

管理制度要求如下：

a） 应对管理活动中的各类管理内容建立安全管理制度，覆盖物理、网络、主机系统、数据、应用、建设和管理等层面的各类管理内容；

b） 应对要求管理人员或操作人员执行的日常管理操作建立操作规程，如系统维护手册和用户操作规程等；

c） 应指定或授权专门的部门或人员负责管理制度的制定；

d） 应组织相关人员对制定的管理制度进行论证和审定，并保存评审记录、评审意见；

e） 应将管理制度以某种方式发布到相关人员手中，并进行登记；

f） 应定期或不定期对管理制度进行评审，对存在不足或需要改进的管理制度进行修订，并保存评审记录、评审意见。

4.3.2 管理机构

管理机构要求如下：

a) 应设立负责人岗位，并定义负责人的职责；

b) 应设立专门的管理员岗位，包括系统管理员、网络管理员、安全管理员等岗位，并定义各个工作岗位的职责；

c) 应根据各个部门和岗位的职责明确授权审批部门及批准人，对系统投入运行、网络系统接入和重要资源的访问等关键活动进行审批，并保存关键活动的审批过程记录；

d) 应加强与办公信息系统供应方、第三方测试机构等的合作与沟通；

e) 应建立外联单位联系列表，包括单位名称、合作内容、联系人、联系方式等内容；

f) 管理员应负责定期进行系统检查，检查内容包括系统日常运行、网络环境、系统漏洞和数据备份等情况，并保存检查报告。

4.3.3 人员管理

4.3.3.1 人员录用

人员录用要求如下：

a) 应指定或授权专门的部门或人员负责人员录用；

b) 应与被录用人员签署保密协议；

c) 应规范人员录用过程，对被录用人员的身份、背景和专业资格等进行审查，对其所具有的技术技能进行考核，并记录审查内容和审查结果。

4.3.3.2 人员离岗

人员离岗要求如下：

a) 应规范人员离岗过程，及时终止离岗员工的所有访问权限，并保存相关记录；

b) 应取回各种身份证件、钥匙、徽章等以及机构提供的软硬件设备，并保存相关记录；

c) 应做好保密文件交接，销毁相关文件等，并保存相关记录。

4.3.3.3 人员考核

应定期对各个管理岗位的人员进行技术知识、安全技能的考核，并对考核内容和考核结果等内容进行记录。

4.3.3.4 人员培训

应对各类人员进行岗位技能培训和相关技术培训，并对培训周期、培训方式、培训内容等内容进行记录。

4.3.3.5 外部支持人员

外部支持人员要求如下：

a) 外部专业技术支持人员应取得相关信息系统集成商或基础软硬件厂商颁发的技能认证证书；

b) 应确保在外部支持人员访问受控区域前得到授权或审批，并保存授权或审批记录；

c) 外部人员访问受控区域要进行登记，登记内容包括进入时间、离开时间、访问区域、访问设备及陪同人员等。

4.4 外包管理

政府部门采购和使用信息技术外包服务时，应符合 GB/T 32926—2016 的要求。