ICS 35.040
L80

中华人民共和国国家标准

GB/T —XXXX

信息安全技术 政府部门信息安全管理基本要求

Information security techniques – Basic requirements of information security for national department

报批稿

（本稿完成日期：2011.11.14）

XXXX - XX - XX 发布 - XX - XX 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/T1.1-2009 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所，中国软件评测中心

本标准主要起草人：杨建军、罗锋盈、王延鸣、高炽扬、朱璇、唐旺、傅如毅、朴献国

引　　言

本标准规范的编制主要是为指导各级政府部门的信息安全管理工作以及信息安全检查工作，保障政府机关各部门各单位信息和信息系统的安全。

信息安全技术 政府部门信息安全管理基本要求

1 范围

本标准规定了政府部门信息安全管理基本要求，用于指导各级政府部门的信息安全管理工作。本标准中涉及保密工作的，按照保密法规和标准执行；涉及密码工作的，按照国家密码管理规定执行。

本标准适用于各级政府部门，其他单位可以参考使用。

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，仅所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 20984-2007 信息安全技术 信息安全风险评估规范

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 22240-2008 信息安全技术 信息系统安全等级保护定级指南

3 信息安全组织管理

本项要求包括：

a) 应加强领导，落实责任，完善措施，建立健全信息安全责任制和工作机制；

b) 应明确一名主管领导，负责本单位信息安全管理工作，根据国家法律法规有关要求，结合实际组织制定信息安全管理制度，完善技术防护措施，协调处理重大信息安全事件；

c) 应指定一个机构，具体承担信息安全管理工作，负责组织落实信息安全管理制度和信息安全技术防护措施，开展信息安全教育培训和监督检查等；

d) 各内设机构应指定一名专职或兼职信息安全员，负责日常信息安全督促、检查、指导工作。信息安全员应当具备较强的信息安全意识和工作责任心，掌握基本的信息安全知识和技能。

4 日常信息安全管理

4.1 基本要求

本项要求包括：

a) 应制定信息安全工作的总体方针和目标，明确信息安全工作的主要任务和原则；

b) 应建立健全信息安全相关管理制度,加强技术支撑手段建设，提高信息安全管理工作的信息化水平；

c) 应加强对人员、资产、采购、外包等的安全管理，并保证信息安全工作经费投入。

4.2 人员管理

本项要求包括：

a) 应建立健全岗位信息安全责任制度，明确岗位及人员的信息安全责任。重点岗位的计算机使用和管理人员应签订信息安全与保密协议，明确信息安全与保密要求和责任；

b) 应制定并严格执行人员离岗离职信息安全管理规定，人员离岗离职时应终止信息系统访问权限，收回各种软硬件设备及身份证件、门禁卡等，并签署安全保密承诺书；
c) 应建立外部人员访问机房等重要区域审批制度，外部人员须经审批后方可进入，并安排本单位工作人员现场陪同，对访问活动进行记录并留存；
d) 应对信息安全责任事故进行查处，对违反信息安全管理规定的人员给予严肃处理，对造成信息安全事故的依法追究当事人和有关负责人的责任，并以适当方式通报。

4.3 资产管理

本项要求包括：

a) 应建立并严格执行资产管理制度；
b) 应指定专人负责资产管理；
c) 应建立资产台账（清单），统一编号、统一标识、统一发放；
d) 应及时记录资产状态和使用情况，保证账物相符；
e) 应建立并严格执行设备维修维护和报废管理制度。

4.4 采购管理

本项要求包括：

a) 应采购安全可控的信息技术产品和服务,并进行安全性评估；
b) 办公用计算机、服务器等设备的更新换代中，应采购配备安全可控 CPU、操作系统等的关键软硬件；
c) 公文处理软件、信息安全产品等应采购安全可控产品，信息安全产品应经过国家认证；
d) 接受捐赠的信息技术产品，使用前应进行安全测评，并与捐赠方签订信息安全与保密协议；
e) 不得采购社会第三方认证机构提供的信息安全管理体系认证服务；
f) 信息系统数据中心、灾备中心不得设立在境外。

4.5 外包管理

本项要求包括：

a) 应建立并严格执行信息技术外包服务安全管理制度；
b) 应与信息技术外包服务提供商签订服务合同和信息安全与保密协议，明确信息安全与保密责任，要求服务提供商不得将服务转包，不得泄露、扩散、转让服务过程中获知的敏感信息，不得占有服务过程中产生的任何资产，不得以服务为由强制要求委托方购买、使用指定产品；
c) 信息技术现场服务过程中应安排专人陪同，并详细记录服务过程；
d) 外包开发的系统、软件上线应用前应进行安全测评，要求开发方及时提供系统、软件的升级、漏洞等信息和相应服务；
e) 信息系统运维外包不得采用远程在线运维服务方式；
f) 应将信息技术外包服务安全管理纳入年度信息安全检查范围。

4.6 经费保障

本项要求包括：

a) 应将信息安全设施运行维护、日常信息安全管理、信息安全教育培训、信息安全检查、信息安全风险评估、信息系统等级测评、信息安全应急处置等费用纳入部门年度预算；
b) 应严格落实信息安全经费预算，保证信息安全经费投入。

5 信息安全防护管理

5.1 基本要求

开展信息化建设应按照同步规划、同步建设、同步运行的原则，同步规划、设计、建设、运行、管理信息安全设施，建立健全信息安全防护体系。

5.2 网络边界防护管理

本项要求包括：

a) 非涉密信息系统与互联网及其他公共信息网络应实行逻辑隔离，涉密信息系统与互联网及其他公共信息网络应实行物理隔离；
b) 建立互联网接入审批和登记制度，严格控制互联网接入口数量，加强互联网接入口安全管理和安全防护。
c) 应采取访问控制、安全审计、边界完整性检查、入侵防范、恶意代码防范等措施，进行网络边界防护；
d) 应根据承载业务的重要性对网络进行分区分域管理，采取必要的技术措施对不同网络分区进行防护、对不同安全域之间实施访问控制；
e) 应对网络日志进行管理，定期分析，及时发现安全风险。

5.3 信息系统防护管理

本项要求包括：

a) 应按照 GB/T 20984-2007 的要求，定期对信息系统面临的安全风险和威胁、薄弱环节以及防护措施的有效性等进行分析评估；
b) 应综合考虑信息系统的重要性、涉密程度和面临的信息安全风险等因素，按照国家信息安全等级保护相关政策和技术标准规范，对信息系统实施相应等级的安全管理；
c) 应按照 GB/T 22240-2008 的要求，确定信息系统安全保护等级；
d) 应按照 GB/T 22239-2008 的要求；对信息系统实施相应等级的安全建设和整改；
e) 应按照信息系统安全等级保护测评相关要求，对信息系统进行等级测评。

5.4 门户网站防护管理

本项要求包括：

a) 应使用“gov.cn”、“政务.cn”或“政务”域名；
b) 网站开通前，应组织专业技术机构进行安全测评，对新增应用要进行安全评估；
c) 应定期对网站链接进行安全性和有效性检查；
d) 应采取必要的技术措施，提高网站防篡改、防攻击能力，加强网站敏感信息保护。
e) 应建立完善网站信息发布审核制度，明确审核程序，严格审核流程。

5.5 电子邮件防护管理

本项要求包括：

a) 应加强电子邮箱系统安全防护，采取反垃圾邮件等技术措施；
b) 应规范电子邮箱注册管理，原则上只限于本部门工作人员注册使用；
c) 应严格邮箱账户及口令管理，采取技术和管理措施确保口令具有一定强度并定期更换。

5.6 终端计算机防护管理

本项要求包括：

a) 应采用集中统一管理方式对终端计算机进行管理，统一软件下发，统一安装系统补丁，统一实施病毒库升级和病毒查杀，统一进行漏洞扫描；
b) 应采取必要的技术手段，规范和加强终端计算机使用行为管理；
c) 应规范软硬件使用，不得擅自更改软硬件配置，不得擅自安装软件；
d) 应加强账户及口令管理，使用具有一定强度的口令并定期更换；
e) 应对接入互联网的终端计算机采取控制措施，包括实名接入认证、IP 地址与 MAC 地址绑定等；
f) 应定期对终端计算机进行安全审计；
g) 非涉密计算机不得存储和处理国家秘密信息。

5.7 存储介质防护管理

本项要求包括：

a) 应严格存储阵列、磁带库等大容量存储介质的管理，采取技术措施防范外联风险，确保存储数据安全；
b) 应对移动存储介质进行集中统一管理，记录介质领用、交回、维修、报废、销毁等情况；
c) 非涉密移动存储介质不得存储涉及国家秘密的信息，不得在涉密计算机上使用；
d) 移动存储介质在接入本部门计算机和信息系统前，应当查杀病毒、木马等恶意代码；
e) 应配备必要的电子信息消除和销毁设备，对变更用途的存储介质要消除信息，对废弃的存储介质要进行销毁。

6 信息安全应急管理

本项要求包括：

a) 应建立健全信息安全应急工作机制，提高应对信息安全事件的能力，预防和减少信息安全事件造成的损失和危害；
b) 应制定信息安全事件应急预案，原则上每年评估一次，并根据实际情况适时修订；
c) 应组织开展应急预案的宣贯培训，确保相关人员熟悉应急预案；
d) 每年应开展信息安全应急演练，检验应急预案的可操作性，并将演练情况报信息安全主管部门；
e) 应建立信息安全事件报告和通报机制，提高预防预警能力；
f) 应明确应急技术支援队伍，做好应急技术支援准备；
g) 应做好信息安全应急物资保障，确保必要的备机、备件等资源到位；
h) 应根据业务实际需要对重要数据和业务系统进行备份。

7 信息安全教育培训

本项要求包括：

a) 应加强信息安全宣传和教育培训工作，提高信息安全意识，增强信息安全基本防护技能；
b) 应建立信息安全教育培训制度，把信息安全教育作为工作人员上岗、干部培训、业务学习的重要内容；
c) 应定期开展信息安全管理人员和技术人员专业技能培训，提高信息安全工作能力和水平；
d) 应把信息安全防护基本技能纳入工作考核范围，并作为干部任用的重要条件；
e) 应记录并保存信息安全教育培训、考核情况和结果。

8 信息安全检查

本项要求包括：

a) 应认真组织开展信息安全检查工作，掌握信息安全总体状况和面临的威胁，查找安全隐患，堵塞安全漏洞，完善安全措施，减少安全风险，提高安全防护能力；

b) 应每年进行一次全面的信息安全检查，重点检查办公系统、业务系统、门户网站的安全防护情况；

c) 应加强检查工作组织领导，建立检查工作责任制，制定检查工作方案并认真落实；

d) 应重视安全技术检测，采取必要的技术检测手段对信息系统、门户网站、服务器、终端设备、终端计算机等进行安全检测。可根据需要委托符合要求的检测机构进行技术检测；

e) 应加强安全检查过程中的保密管理和风险控制，严格检查人员、有关文档和数据的安全保密管理，制定安全检查应急预案，确保被检查信息系统的正常运行；

f) 应对安全检查中发现的问题进行分析研判，制定整改措施并及时整改；

g) 应对年度安全检查情况进行全面总结，按照要求如实完成检查报告并报信息安全主管部门。

参 考 文 献

[1] GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求
[2] GB/T 20270-2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20282-2006 信息安全技术 信息系统安全工程管理要求
[4] 国保发[2007]13 号 关于印发《关于加强党政机关计算机信息系统安全和保密管理的若干规定》的通知
[5] 国信办[2006]5 号 关于开展信息安全风险评估工作的意见
[6] 公通字[2007]43 号 关于印发《信息安全等级保护管理办法》的通知
[7] 公信安[2007]861 号 关于开展全国重要信息系统安全等级保护定级工作的通知
[8] NIST FIPS-200:，联邦信息与信息系统最小安全要求
[9] NIST SP 800-53:2002 联邦信息系统推荐安全控制
[10] 工信部联协[2010]394 号 关于加强信息安全管理体系认证安全管理的通知
[11] 财库[2010]48 号 关于信息安全产品实施政府采购的通知
[12] 国办发[2010]47 号 国务院办公厅关于进一步做好政府机关使用正版软件工作的通知