ICS 35.020
L70
备案号:40354-2014

DB11

北　京　市　地　方　标　准

DB11/T 1041—2013

政务办公终端安全管理规范

Security management specification for government office computer

2013 - 12 - 20 发布　　2014 - 04 - 01 实施

北京市质量技术监督局　　发布

目　　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由北京市经济和信息化委员会提出并归口。

本标准由北京市经济和信息化委员会组织实施。

本标准起草单位：北京信息安全测评中心、北京市统计局信息中心、北京东祥骏昌科技有限公司。

本标准主要起草人：刘海峰、钱秀槟、王春佳、黄少青、赵章界、张晓梅、梁博、李晨旸、贺海、史蓉、李晓燕。

政务办公终端安全管理规范

1 范围

本标准规定了政务办公终端的安全管理原则、安全管理要求、软件配置基本要求和外围控制基本要求。

本标准适用于政务办公终端，不适用于处理涉及国家秘密信息的计算机终端。

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 25069-2010 信息安全技术 术语

3 术语、定义和缩略语

3.1 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。

政务办公终端 government office computer

用于处理涉及政务工作的台式、便携式微型计算机系统，不包含移动智能终端（如掌上电脑、智能手机等）。

3.2 缩略语

下列缩略语适用于本标准：

IP	网络之间互连的协议	Internet Protocol
MAC	介质访问控制	Media Access Control

4 安全管理原则

4.1 明确责任

政务办公终端的主管单位、运维单位和使用者应按照“谁主管谁负责、谁运行谁负责、谁使用谁负责”的原则明确安全责任。

4.2 综合防范

进行政务办公终端安全管理时，应全面综合考虑操作系统软件、应用软件、网络接入、外联控制、安全审计等各个层面对政务办公终端安全的影响。

4.3 适度保护

应根据政务办公终端处理信息的重要程度给予相应的保护。本标准规定了政务办公终端的基本安全防护要求，对安全有更高要求的政务办公终端应符合附录A中对应的安全增强要求。

5 安全管理要求

5.1 责任人员

5.1.1 岗位

5.1.1.1 明确一名主管领导，负责政务办公终端安全管理的领导和协调工作。

5.1.1.2 明确政务办公终端安全管理的责任部门和岗位，并在部门和岗位职责中明确相应的责任。岗位职责应包含本单位政务办公终端的安全配置、日常维护以及定期的安全检查工作。

5.1.2 培训

5.1.2.1 用于政务办公终端的软件要制定配套的安装、配置及使用等操作手册，按需求组织宣贯培训，指导用户正确使用。

5.1.2.2 结合本单位信息化工作实际情况，组织内部和外部培训，包括但不限于信息化相关法律法规的宣贯、信息安全意识培训、信息化和信息安全常识和基础技能的培训等。

5.2 软件管理

5.2.1 根据日常业务需求，建立政务办公终端软件选用列表，提供支撑业务开展所必需的政务办公终端软件。列表应包含系统软件和应用软件等类别，其中系统软件可包括操作系统、系统补丁等；应用软件可包括输入法软件、文档编辑软件、文件压缩软件、网页浏览软件、邮件客户端软件、文件阅读器、图片查看、媒体播放、安全防护软件以及打印机等办公设备驱动程序等。根据部门业务需要还可包括财务软件、远程管理软件以及专用业务系统客户端等。

5.2.2 应依照政务办公终端软件选用列表，采用正版软件，建立软件资产清单。

5.2.3 对政务办公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。

5.3 安全制度

5.3.1 信息安全工作总体方针和安全策略中应包含政务办公终端安全。

5.3.2 对政务办公终端软件安全管理活动中重要的管理内容建立安全管理制度；对安全管理人员或操作人员执行的重要政务办公终端软件管理操作建立操作规程。

5.3.3 通过正式有效的方式将管理制度和操作规程发布。

5.3.4 建立政务办公终端软件安装和变更的审批制度。因工作需要在政务办公终端中增加或减少安装的软件、对软件进行升级、或变更软件配置前，应按照审批流程进行审核，经审核批准并备案后，由责任部门或责任人对相关政务办公终端实施软件变更或监督实施软件变更。变更完成后，应及时更新软件配置清单。

6 软件配置基本要求

6.1 操作系统配置要求

6.1.1 安装配置

6.1.1.1 按照统一规则为政务办公终端命名，名称应易于识别。

6.1.1.2 根据日常业务需求确定需要的组件和服务，仅安装支撑业务开展所必需的系统组件和服务。

6.1.2 账号配置

6.1.2.1 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。
6.1.2.2 删除或禁用系统中的特殊账号、无用账号。

6.1.3 口令配置

6.1.3.1 设置账号口令保护机制，不应使用空口令账号登录系统。
6.1.3.2 账号口令应由字母、数字及特殊字符组成，长度应不少于6位。
6.1.3.3 重要账号口令应不少于8位。

6.1.4 日志配置

6.1.4.1 设置系统日志审计，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。
6.1.4.2 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。
6.1.4.3 系统日志保留时间应不少于7天。

6.1.5 安全配置

6.1.5.1 关闭默认共享，明确共享文件夹的共享权限。
6.1.5.2 关闭移动存储介质的自动播放功能。
6.1.5.3 禁用远程桌面服务。
6.1.5.4 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。
6.1.5.5 启用补丁自动更新功能。
6.1.5.6 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。

6.2 应用软件配置要求

6.2.1 一般要求

6.2.1.1 根据政务办公终端软件选用列表，按照最小需求安装应用软件及相关组件。
6.2.1.2 在政务办公终端操作系统中设置固定的应用程序安装目录、数据临时存储目录。应用程序应集中安装在应用程序安装目录中；对于存在临时文件的应用程序，应在数据临时存储目录中建立独立的子目录，用于保存该程序的临时文件或缓存文件。

6.2.2 文档编辑软件配置

6.2.2.1 文档编辑软件应设置用于标识用户的基本信息。
6.2.2.2 限制文档编辑软件自动批量处理功能。
6.2.2.3 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。
6.2.2.4 启用文档定时保存功能。

6.2.3 网页浏览器配置

6.2.3.1 网页浏览器应设置统一、可信的初始页面或设置为空白页。

6.2.3.2 设置下载文件的统一存储目录，存储目录应为数据临时存储目录中的独立子目录。

6.2.3.3 设定本地缓存空间大小，并定期清理本地缓存、历史记录以及临时文件内容。

6.2.3.4 根据需要建立浏览器插件或组件列表。

6.2.3.5 及时对所有下载资源进行恶意代码扫描。

6.2.4 邮件客户端配置

6.2.4.1 针对不同的邮箱账号，应设置易识别的账号标识信息。

6.2.4.2 设置邮箱账户的访问口令，邮箱账户口令应不同于系统口令，并定期更新，口令更新周期应不超过3个月。

6.2.4.3 建立独立于应用程序安装目录之外的独立目录，用于存储已接收、已发送及分类保存的邮件。

6.2.4.4 禁用或限制邮件客户端软件对带格式邮件、附件的自动处理或显示功能。

6.2.4.5 及时对邮件附件进行恶意代码扫描。

6.2.4.6 定期清除、转移或归档已收取的邮件，避免信息泄露。

6.2.5 安全防护软件配置

6.2.5.1 设置为开机自动启动方式。

6.2.5.2 设置对本机数据进行定期安全扫描。

6.2.5.3 设置对接入介质进行自动安全扫描。

6.2.5.4 启用软件及特征库的自动更新功能。

6.2.5.5 启用政务办公终端的防火墙，并以白名单的方式设置访问控制规则。

7 外围控制基本要求

7.1 准入控制要求

7.1.1 网络规划

根据各部门工作职能和处理业务的重要程度，划分不同的子网，按照方便管理控制和安全隔离的原则为各子网分配IP地址段。

7.1.2 网络准入

设置并启用政务办公终端准入控制策略，通过物理接入点或政务办公终端MAC地址等物理因素，将政务办公终端接入到指定的物理子网或逻辑子网中。

7.1.3 介质接入

设置并启用移动存储介质接入控制策略，自动实行存储数据安全性扫描。

7.2 流量监控要求

7.2.1 流量监控配置

设置并启用网络流量监控策略，实时监测网络带宽使用等情况，能对指定子网中的政务办公终端带宽使用进行限制。

7.2.2 流量内容分析

具备对网络出口、骨干链路等关键部位网络流量进行分析的能力，能根据特征监测发现典型的网络攻击、恶意软件传播等行为。

附 录 A
（规范性附录）
政务办公终端安全增强要求

A.1 四类安全增强要求说明

A.1.1 自动化管理型

以实现自动化管理、提高政务办公终端管理效率为重点，使政务办公终端实时有效运行、数据实时可用，解决管理政务办公终端数量过大或政务办公终端管理人员过少等问题。

A.1.2 数据保护型

以保护政务办公终端数据为重点，使政务办公终端用于处理敏感信息、访问涉及敏感信息的重要系统时，数据不被恶意泄露和篡改，解决将政务办公终端数据保护性放在首位的情况。

A.1.3 监控审计型

以规范政务办公终端用户操作为重点，能及时发现安全问题以及事后定位信息安全事件，能实时监测政务办公终端软件使用行为，在发生安全事件后能为管理人员提供有效的网络访问行为和内容审计记录。

A.1.4 外设可控型

以加强政务办公终端外设控制力度为重点，使政务办公终端在安全、可信、可控的网络环境中运行。

A.1.5 增强要求选择

政务办公终端安全管理的责任部门或人员可根据本单位的安全管理实际需求，在满足基本要求的基础上，选择上述四类增强要求中的一类或几类安全增强要求的组合。

A.2 自动化管理型增强要求

A.2.1 操作系统要求

A.2.1.1 在政务办公终端上安装同一类型操作系统。
A.2.1.2 在操作系统安装时统一系统恢复设置。

A.2.2 终端管理系统要求

部署统一的终端管理系统，实现对所管辖终端的自动化管理。管理的内容应至少包括：资产管理、状态监测、系统补丁分发、软件安装管理、主机访问控制、远程管理等。

A.2.3 安全防护软件要求

设置安全防护软件统一管理，实现恶意代码防范规则库自动、集中、定时更新。

A.3 数据保护型增强要求

A.3.1 软件维护管理要求

定期对安全域中的网络设备、政务办公终端进行安全扫描，及时发现可能的安全隐患。

A.3.2 账号安全要求

A.3.2.1 不应直接使用系统管理员账号。
A.3.2.2 多个用户不应共同使用一个账号登录操作系统。
A.3.2.3 账号口令应与其它的鉴别方式（如动态口令、数字证书等）配合使用。
A.3.2.4 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。
A.3.2.5 账号口令应定期更换，更换周期应不超过3个月。
A.3.2.6 设置口令延时、尝试次数阈值，达到阈值时应采取响应措施，防范暴力口令破解。

A.3.3 系统日志要求

设置日志文件大小及达到设定值或无存储空间时的操作方式。

A.3.4 文档编辑软件要求

A.3.4.1 禁用文档编辑软件的网络功能。
A.3.4.2 限制文档编辑软件在本地保存副本或临时文件。
A.3.4.3 重要文档设置口令保护，限制对文档的读写权限。

A.3.5 网页浏览器要求

A.3.5.1 禁用本地缓存网页文件。
A.3.5.2 禁用本地自动保存用户账号、口令等敏感信息。

A.3.6 主机防护要求

A.3.6.1 操作系统及应用软件的补丁程序在安装前应进行测试。
A.3.6.2 统一安装恶意软件防范工具，定期更新恶意软件特征库。
A.3.6.3 对本地重要文件进行保护，保障文件的保密性和完整性。

A.3.7 准入控制要求

A.3.7.1 对接入安全域的政务办公终端进行认证，通过验证后方可使用网络资源。
A.3.7.2 对未授权政务办公终端接入及安全域内政务办公终端未授权外联进行限制。
A.3.7.3 能够对内部网络的内部用户未通过准许私自联到外部网络的行为进行检查。

A.3.8 外设管理要求

加强移动存储介质的管理，检验接入介质的合法性，并进行必要的审计。

A.4 监控审计型增强要求

A.4.1 基础要求

A.4.1.1 建立独立于政务办公终端的监控和审计系统。

A.4.1.2 在核心交换机设置端口镜像，或采取其他有效措施，将所有网络流量数据发送至监控和审计系统。

A.4.2 策略设置要求

A.4.2.1 依照政务办公终端软件运行需求，设置并启用软件进程监测策略，对违反策略的行为进行限制。

A.4.2.2 依照政务办公终端软件选用列表，设置并启用重要软件日志审计策略，对软件增加、修改、删除等软件变更情况进行审计，审计信息应包括日期、时间、来源、用户、操作、结果等要素。

A.4.2.3 设置审计数据保存应不少于60天，数据保存应独立于被保护政务办公终端之外。

A.4.3 日志记录要求

A.4.3.1 将日志记录通过网络远程保存在外部日志服务器中。

A.4.3.2 日志记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息，并对违反策略的访问行为及时响应和处置。

A.4.3.3 审计记录应独立保存，保存时间应不少于60天。

A.5 外设可控型增强要求

设置并启用政务办公终端外联控制策略，未经授权不应通过任何形式连接外部网络,不应使用USB接口为手机等外部设备充电，并对政务办公终端未经授权的外联行为进行监测和处置。