白山市中级人民法院信息化标准

（试行）

二〇二二年十一月

目 录

引　言

随着信息化建设的不断推进，各级政府部门充分认识到信息系统在国家各行业各层面的重要性，把信息安全上升到事关国家安全的地位。为了保护我国的基础信息网络和重要信息系统，推出信息安全等级保护制度，并作为国家信息安全保障工作的基本制度。

1994 年，中华人民共和国计算机信息系统安全保护条例(国务院 147 号令)明确提出国家实行信息安全等级保护制度。1999 年，国家制定了国家标准《计算机信息系统安全保护等级划分准则（GB17859-1999)》。2003 年，中办国办 27 号文明确提出实施等级保护作为国家信息安全工作的重点工作之一，随后国家制定发布了一系列等级保护相关标准。近来国家密集出台了等级保护管理办法和定级工作的政策，在全国推广重要信息系统定级工作。2007 年 6 月 22 日，公安部、国家保密局、国家密码管理局、国务院信息化工作办公室联合发布“信息安全等级保护管理办法”（公通字[2007]43 号），就等级划分与保护、等级保护的实施与管理等作出了明确规定。

在 2014 年的 2 月 27 日，中央网络安全和信息化领导小组宣告成立，在北京召开了第一次会议。中共中央总书记、国家主席、中央军委主席习近平亲自担任组长，李克强、刘云山任副组长，再次体现了中国最高层全面深化改革、加强顶层设计的意志，显示出在保障网络安全、维护国家利益、推动信息化发展的决心。

2017 年 6 月 1 日，《中华人民共和国网络安全法》正式施行。为保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，国家已将网络安全上升到法律层面，真正做到有据可依有法可循。

2016 年 2 月下发的《人民法院信息化建设五年发展规划（2016-2020)》中，对加强安全体系建设，提高安全保护水平有着明确的要求。同时为落实《人民法院信息化“十三五”发展规划》，推进人民法院信息安全保障体系建设，最高院制定并下发了《人民法院信息安全保障总体建设方案》，参照上述相关要求，结合我省法院信息系统建设的实际情况，特制定吉林省法院信息安全建设标准。

1 范围

本标准从安全技术和安全管理两方面规定了法院系统信息安全建设基线要求。

本标准适用于各级人民法院按信息安全等级保护要求，进行新建法院信息系统的安全规划、设计、建设、管理和运行控制以及已投入运行信息系统的安全整改和运行控制。

2 规范性引用文件

国家信息安全相关文件：

- 《中华人民共和国网络安全法》
- 《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）
- 《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）
- 《关于信息安全等级保护工作的实施意见》（公通字[2004]66 号）
- 《信息安全等级保护管理办法》（公通字[2007]43 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》（公信安[2007]861 号）
- 《公安机关信息安全等级保护检查工作规范》（公信安[2008]736 号）
- 《关于开展信息安全等级保护安全建设整改工作的指导意见》（公信安[2009]1429 号）
- 《关于推动信息安全等级保护测评体系建设和开展等级测评工作的通知》（公信安[2010]303 号）

国信安标委组织制定的国家标准：

- GB/T22240-2008《信息安全技术 信息系统安全保护等级定级指南》
- GB17859-1999《计算机信息系统 安全保护等级划分准则》
- GB/T22239-2008《信息安全技术 信息系统安全等级保护基本要求》
- GB/T25070-2010《信息安全技术 信息系统等级保护安全设计技术要求》
- GB/T20269-2006《信息安全技术 信息系统安全等级保护管理要求》

- GB/T20270-2006《信息安全技术 网络基础安全技术要求》
- GB/T20271-2006《信息安全技术 信息系统通用安全技术要求》
- GB/T20272-2006《信息安全技术 操作系统安全技术要求》
- GB/T20273-2006《信息安全技术 数据库管理系统安全技术要求》
- GB/T20282-2006《信息安全技术 信息系统安全工程管理要求》
- GB/T21082-2007《信息安全技术 服务器安全技术要求》
- GB/T 28448-2012《信息安全技术 信息系统安全等级保护测评要求》
- GB/T 28449-2012《信息安全技术 信息系统安全等级保护测评过程指南》

最高人民法院指导文件：

- 《人民法院非涉密重要信息系统安全等级保护定级工作指导意见》
- 《关于进一步推进人民法院信息安全等级保护工作的通知》
- 《全国法院计算机信息网络建设管理暂行规定（试行）》
- 《人民法院信息网络系统建设技术规范》
- 《人民法院信息化“十三五”发展规划》
- 《人民法院信息安全保障总体建设方案》

3 技术标准

3.1 物理安全

3.1.1 物理位置选择

本项要求包括：

a) 机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；各中院、基层院已经建设完毕的机房要通过其他建筑加固措施确保具备该能力。

b) 机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

3.1.2 物理访问控制

本项要求包括：

a） 机房出入应安排专人管理，控制、鉴别和记录进入的人员；

b） 需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；要求制定机房出入管理制度，制度中必须要求进出机房需要申请和审批流程，并在执行制度的过程中留存记录，记录保存时间不低于6个月。

c） 应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；

d） 重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。要求机房配备可审计出入痕迹的门禁系统，审计记录保存时间不低于6个月。

3.1.3 防盗窃和防破坏

本项要求包括：

a） 应将主要设备放置在机房内；

b） 应将设备或主要部件进行固定，并设置明显的不易除去的标记；标识标签应清晰记录系统名称，IP地址，负责人，所在网络区域等信息，必要时，可通过颜色区域进行划分。

c） 应将线缆进行规范化铺设，可铺设在地下桥架内或上走线桥架中；

d） 应对介质分类标识，存储在介质库或档案室中；应配备专业密码文件柜对介质进行保存。

e） 应利用光、电等技术设置机房防盗报警系统；机房监控系统必须具备布防、防盗报警能力。

f） 应对机房设置监控报警系统。

3.1.4 防雷击

本项要求包括：

a） 机房建筑应设置避雷装置；

b） 应设置防雷保安器，防止感应雷；

c） 机房应设置交流电源地线。

3.1.5 防火

参考最高院发布的《法院审判业务综合楼信息化建设指南》要求建设，本项重点包括：

a） 机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；
b） 机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；
c） 机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。

3.1.6 防水和防潮

本项要求包括：

a） 水管安装，不得穿过机房屋顶和活动地板下；
b） 应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；
c） 应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；
d） 应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。

3.1.7 防静电

本项要求包括：

a） 主要设备应采用必要的接地防静电措施；如防静电地网等。
b） 机房应采用防静电地板。

3.1.8 温湿度控制

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。机房必须配备符合本院的机房专用精密空调。

3.1.9 电力供应

参考最高院发布的《法院审判业务综合楼信息化建设指南》要求建设，本项重点包括：

a） 应在机房供电线路上配置稳压器和过电压防护设备；

b） 应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；

c） 应设置冗余或并行的电力电缆线路为计算机系统供电；

d） 应建立备用供电系统。

3.1.10 电磁防护

本项要求包括：

a） 应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；

b） 电源线和通信线缆应隔离铺设，避免互相干扰；

c） 应对关键设备和磁介质实施电磁屏蔽。

3.2 网络安全

3.2.1 结构安全

本项要求包括：

a） 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；必须配备冗余核心交换机。

b） 应保证网络各个部分的带宽满足业务高峰期需要；

c） 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；通过交换机策略的执行。

d） 应绘制与当前运行情况相符的网络拓扑结构图；

e） 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；

f） 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；可通过防火墙、交换机Vlan、ACL等技术实现。

g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。应在网络出口关键位置对业务进行带宽占用等级划分，采用流量控制系统对带宽进行控制。

3.2.2 访问控制

本项要求包括：

a) 应在网络边界部署访问控制设备，启用访问控制功能；网络边界位置必须部署防火墙系统，并配置访问控制策略。

- 中院防火墙性能及功能要求：整机吞吐量≥18Gbps；并发连接数≥400 万；每秒新建连接数≥15 万；电源冗余电源；支持 BYPASS；专用多核处理器、非 X86 硬件架构，Web 界面可显示处理器核心数，且各核心均参与工作。访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源 IP 或者目的 IP 进行连接数控制；必须支持组播 NAT；可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测；具备中国国家认证认可监督管理委员会颁发的《ISO14001：2004（GB/T24001-2004）环境管理体系认证》资质；具有国家信息安全测评中心颁发的《信息安全服务资质证书》安全工程类二级或以上；中国国家信息安全漏洞库 - 技术支撑单位（二级）；具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》。
- 基层院采用满足国标的下一代防火墙，要求详见 3.2.5 入侵防范章节。

b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；防火墙策略细化，禁止采用 any-any 的方式。

c) 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；

d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；必须开启

TCP 会话与安全设备登陆的会话超时功能。

e) 应限制网络最大流量数及网络连接数；防火墙必须开启此功能。

f) 重要网段应采取技术手段防止地址欺骗；重要网段开启 IP 与 MAC 地址绑定策略，必要时可与交换机端口进行三项绑定。

g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；防火墙安全策略细化到单个用户。

h) 应限制具有拨号访问权限的用户数量。

3.2.3 安全审计

本项要求包括：

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；采用网络行为审计、流量控制审计等软硬件进行控制。

b) 审计记录应包括：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；采用专业日志审计设备。

c) 应能够根据记录数据进行分析，并生成审计报表；要求配备的日志审计设备具备报表生成功能，报表具备较好的可读性。

d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。审计记录的管理员账号不应具备删除日志的功能。

e) 各安全审计设备可进行统一管理，审计数据集中存储。并进行大数据分析，省院大数据分析系统要求如下：独立完成审计日志采集，不依赖于设备或系统自身的日志系统；审计工作不影响被审计对象的性能、稳定性或日常管理流程；审计结果存储于分布式存储系统；提供全中文 WEB 管理界面，无需安装任意客户端软件或插件；支持将可视化的数据实时的投影到大屏进行展示；支持分布式部署和集中化管理和升级模式；支持分析超过 100 种协议，如 HTTP、FTP、SMTP、POP3、TFTP、TCP、UDP、NFS、SNMP、ICMP、RTMP、DNS、IRC、SMB、数据库协议（MSSQL、MySQL、Oracle）等；内置 20 多种复杂场景模型，如：扫描攻击、异常流量攻击、DDos 攻击、CC 攻击、恶意访问者攻击、Webshell 攻击、恶意文件攻击、暴力破解攻击、僵尸主机

检测、漏洞利用成功事件、潜伏型应用检测、钓鱼网站检测、web页面篡改检测。支持原始事件追踪溯源、告警事件追踪溯源、、安全事件追踪溯源、支持攻击者追踪溯源；全局态势感知可视化；支持攻击者黑白名单；支持与专业的流量解析设备进行深度对接、精确识别1000+种应用协议；支持不同扫描器交叉验证；支持自动发现隐藏不受控的资产；支持对漏洞信息进行标准化，提供结论性的分析结果；支持弱点全生命周期管理，从发现、修复、再确认到关闭；支持弱点趋势分析；支持漏洞修复率、资产覆盖率等多维度分析和展现；支持告警处置建议；支持网络拓扑的可视化告警。

f) 为确保统一管理与兼容性分析，各中院基层院要求配备专业的日志审计、运维审计（堡垒机）类设备，并按照如下要求进行配置：

- 中院日志审计性能及功能要求：要求支持50个审计日志源，产品采用CF卡启动；产品支持分布式部署，支持集中式管理和升级模式；产品采用B/S架构操作方式，无需客户端安装，支持监控设备自身CPU、内存、磁盘等工作运行状况；产品采用解决方案包上传对产品进行功能扩展，无需要代码开发；支持常见的虚拟机环境日志收集，包括Xen、VMWare、Hyper-V等；支持基于内存的实时关联分析，跨设备的多事件关联分析；支持自定义条件都事件进行聚合；进行关联分析的规则可定制；支持根据资产价值、资产漏洞、针对漏洞的威胁事件三者进行威胁的自动关联分析（三维关联），所有的三维关联算法和准则以CVE、Bugtraq、OWASP公开协议和标准为为基础；支持日志备份自动传送到远程服务器；极高的日志高查询性能，支持亿级的日志里根据做任意的关键字及其它的检索条件,在秒级里返回查询结果；内置合规性报表1000+种，内置SOX、ISO27001、WEB安全等解决方案包，内置完善的等级保护合规报表；日志审计提供评分系统；注册用户资产时，提供自动发现识别能力，提供一键式故障排除功能；信息系统安全产品销售许可证；提供公安部信息安全产品检测中心出具产品检验报告，报告需符合《信息安全技术日

志分析产品检验规范》，并提供完整的检测报告复印件（行标三级）；涉密信息系统产品检测证书；计算机软件著作权登记证书；

- 基层院日志审计性能及功能要求：要求支持 20 个审计日志源，其他功能同中院要求。
- 中院运维审计（堡垒机）性能及功能要求：最大资产数 200 个；最大字符连接 200 个；最大图形连接 30 个；产品为自主知识产权，非 OEM；系统须安装在专用的 CF 卡中，审计数据存储在磁盘中，防止操作系统故障导致审计数据丢失；每个部门可以管理本部门及下级部门的用户角色：部门管理员、配置管理员、审计管理员、普通用户；每个部门的审计管理员可以管理本部门及下级部门的运维会话日志；支持手机 APP 动态口令认证方式登录堡垒机，且新用户首次登录后需强制绑定 APP 动态口令；基于不同的用户设置不同的双因子认证模式，如 user1 用动态令牌、user2 用 USBkey、user3 手机 APP 动态口令认证；支持认证方式的全局设置：可以选择启用哪种或者哪几种认证登录窗口；具备公安部销售许可证；软件著作权证书；国家涉密产品资质证书；中国信息安全认证中心 ISCCC 认证；
- 基层院运维审计（堡垒机）性能及功能要求：最大资产数 100 个；最大字符连接 100 个；最大图形连接 20 个；，其他功能同中院要求。

3.2.4 边界完整性检查

本项要求包括：

a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；要求配备安全准入控制网关，可通过与接入交换机或者终端管理软件配合实现安全准入的控制。

b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。要求配备具备限制非法外联功能的终端管理软件。

3.2.5 入侵防范

本项要求包括：

a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；要求在网络边界处配备入侵防御设备。

b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。

c) 入侵检测及防范设备能够进行统一管理，攻击行为记录能够进行集中存储。

- 中院入侵防范性能及功能要求：吞吐量≥3Gbps，并发连接数≥300W，每秒新建连接数≥5W；集成第三方专业防病毒厂商的专业病毒库，特征规则数量不少于 10000 条；支持识别主流文件共享：支持应用包括 FTP 类文件传输、Gbridge、SMB、NFS、bonpoo、boxnet、SVN、Hamachi、ISCSI、Clip2Net 等；可以在 IPv4/IPv6 双栈、MPLS 等复杂网络环境下良好的工作，可以识别并检测 QinQ、PPPoE、MPLS、GRE、Vlan 等特殊封装的网络报文，具备面向下一代网络的各种特性；系统应具备地址簿功能，在报表中可直观显示所有攻击事件的攻击源 IP 所处省份或某个运营商等信息；具备国家保密局《涉密信息系统产品检测证书》；具备中国信息安全认证中心颁发的《信息安全应急处理一级》资质；具备中国信息安全认证中心颁发的《信息安全风险评估服务一级》资质；具备中国国家认证认可监督管理委员会颁发的《ISO14001：2004（GB/T24001-2004）环境管理体系认证》资质；具备中国国家认证认可监督管理委员会颁发的《ISO27001 信息安全管理体系认证》资质；具备通信企业协会颁发的《风险评估一级》资质；
- 基层院必须选用满足国标的下一代防火墙，性能及功能要求：整机吞吐量≥15Gbps；并发连接数≥300 万；每秒新建连接数≥10 万；电源冗余电源；支持 BYPASS；提供防病毒功能模块和 IPS 功能模块；专用多核处理器、非 X86 硬件架构，Web 界面可显示处理器核心数，

且各核心均参与工作。访问控制策略支持基于源/目的 IP，源/目的端口，源/目的区域，用户（组），应用/服务类型的细化控制方式；支持 IPv4 / v6 NAT 地址转换，支持源目的地址转换，目的地址转换和双向地址转换，支持针对源 IP 或者目的 IP 进行连接数控制；必须支持组播 NAT；可提供最新的威胁情报信息，官方网站每周会进行安全通告，能够对新爆发的流行高危漏洞进行预警和自动检测；具备中国国家认证认可监督管理委员会颁发的《ISO14001：2004（GB/T24001-2004）环境管理体系认证》资质；具有国家信息安全测评中心颁发的《信息安全服务资质证书》安全工程类二级或以上；中国国家信息安全漏洞库－技术支撑单位（二级）；具有中国国家保密局测评中心颁发的《涉密信息系统产品检测证书》。

3.2.6 恶意代码防护

本项要求包括：

a) 应在网络边界处对恶意代码进行检测和清除；

b) 应维护恶意代码库的升级和检测系统的更新。

- 各中院、基层院安装支持统一管理的防病毒产品，具体要求如下：产品获国家公安部销售许可证；所有产品必须是自主开发，拥有自主知识产权。厂商必须在国内有独立的监控中心。厂商在国内、国外分别有独立的研发中心。厂商在国内、国外分别有独立的病毒响应中心。通过中国信息安全评测认证中心的《信息安全服务资质标准》的信息安全服务一级资质认证。防病毒产品通过第三方专业机构 AV-Test 和 NssLab 测试并且最终评测结果在前 3 名；具备病毒爆发防御功能。当最新病毒爆发时，可在病毒代码未完成之前自动对企业网络中的病毒传播端口、共享等进行关闭，切断病毒传播途径，预防最新病毒的攻击；具备 Web 信誉评估功能，包含 HTTPS 通信扫描，结合云安全架构自动识别并屏蔽恶意站点，阻止病毒自动更新；支持与微软 AD 的集成，可套用 AD 的分组方式，方便管理，可分配 AD 的组和用户不同的服务器管理权限，可监视和管理 AD 内计算机的安

全状态；利用初始母版和白名单技术，记录扫描的缓存文件，从而缩短虚拟桌面的扫描时间；具备病毒源准确定位功能，快速查获病毒出处（Virus/Malware Logs 里有一列“Infection Source”）；管理端病毒代码及引擎升级可通过多种方式，如直接通过 Internet；通过升级工具直接升级以满足大多内网用户升级的需要（TMUT）；能够有效防御高级持续威胁（APT）的攻击，通过联动机制禁止客户机对命令与控制服务器的外联；必须具备终端位置感知功能，针对客户端处于内、外网能够部署不同的策略。

- 各中院、基层院配备威胁发现系统性能及功能要求如下：产品能够进行统一管理；吞吐量不低于 250 Mbps；最高并发连接不低于 16,000；产品中所用的防病毒引擎，病毒代码，防病毒扫描原理都必需为厂商自有技术，非 OEM 或引入其他厂商技术，以保证服务支持的连续性，和技术维护的一贯性；产品获国家公安部销售许可证；所有产品必须是自主开发，拥有自主知识产权；国产软件登记证；可扫描网络第 2 层至第 7 层数据流量；可选择特定协议或 IP 地址自定义检测；支持自定义 IP 地址、URL、域名与文件的访问监控；支持超过 100 种协议，如 HTTP、FTP、SMTP、POP3、TFTP、TCP、UDP、NFS、SNMP、ICMP、RTMP、DNS、IRC、SMB、数据库协议（MSSQL、MySQL、Oracle）等；能够侦测各种文件型病毒，如木马、僵尸、后门等；″1. 可侦测识别 iOS、赛班、安卓、微软等移动设备；可与移动应用信誉系统（MRS）联动，侦测安卓系统的恶意应用 App；威胁流量与协议异常检测 ，如零日攻击、网络蠕虫、木马、后门、僵尸、间谍软件、网络漏洞、网页威胁（网页漏洞、跨网站攻击）、钓鱼邮件、暴力攻击、数据库注入攻击等。

3.2.7 网络设备防护

本项要求包括：

a) 应对登录网络设备的用户进行身份鉴别；

b) 应对网络设备的管理员登录地址进行限制；

c） 网络设备用户的标识应唯一；

d） 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；

e） 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；

f） 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；

g） 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；

h） 应实现设备特权用户的权限分离。

3.2.8 安全系统升级

各级人民法院应按照实际使用的数量对网络安全设备定期进行升级。包括：统一安全网关设备、威胁发现检测系统、防火墙、入侵防御、各类审计设备、其他安全设备等。

3.3 主机安全

3.3.1 身份鉴别

本项要求包括：

a） 应对登录操作系统和数据库系统的用户进行身份标识和鉴别；重要业务系统应采用双因子认证。

b） 操作系统和数据库系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；口令应设置8位以上数字字母特殊字符两种以上组合，每月更换一次。

c） 应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；通过操作系统组策略、安全设备登录失败限制功能进行控制。

d） 当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；要求通过运维审计系统进行远程管理。

e） 应为操作系统和数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性。

f） 应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。应采用用户名密码、电子证书、动态令牌、USBKEY等方式进行组合。

3.3.2 访问控制

本项要求包括：

a） 应启用访问控制功能，依据安全策略控制用户对资源的访问；

b） 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；

c） 应实现操作系统和数据库系统特权用户的权限分离；

d） 应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；

e） 应及时删除多余的、过期的帐户，避免共享帐户的存在。

f） 应对重要信息资源设置敏感标记；

g） 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

3.3.3 安全审计

本项要求包括：

a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户；应配备专用的日志审计、运维审计、数据库审计等设备。

b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

c） 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

d） 应能够根据记录数据进行分析，并生成审计报表；

e） 应保护审计进程，避免受到未预期的中断；

f） 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

g） 审计设备可进行统一管理，审计数据支持集中存储。

3.3.4 剩余信息保护

本项要求包括：

a） 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b） 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

3.3.5 入侵防范

本项要求包括：

a） 应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；

b） 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；

c） 操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。应利用内网安全系统对补丁进行管理。

d） 入侵检测及防范设备能够进行统一管理，攻击行为记录能够集中存储。

3.3.6 恶意代码防范

本项要求包括：

a） 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；

b） 主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；

c） 应支持防恶意代码的统一管理。

3.3.7 资源控制

本项要求包括：

a） 应通过设定终端接入方式、网络地址范围等条件限制终端登录；对运维审计系统、防火墙等关键设备应限制管理主机IP地址。

b） 应根据安全策略设置登录终端的操作超时锁定；要求设置屏幕保护恢复时启用密码锁定功能，时间设置为1分钟。

c） 应对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；应通过运维管理软件对服务器的资源占用情况进行实时监控。

d） 应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。应在运维管理软件上对系统的关键指标设定监控阀值，并在超过阀值时进行报警。

e） 运维管理系统所监控的资源数据能够进行集中管理。

3.3.8 安全系统升级

a） 各级人民法院应按照实际使用的数量对主机安全防护系统定期进行升级。包括：客户端防病毒系统、服务器防病毒系统、内网安全管理系统、其他安全系统等。

b） 防病毒系统、内网安全管理系统终端覆盖及升级率达到100%。

3.4 应用安全

3.4.1 身份鉴别

本项要求包括：

a） 应提供专用的登录控制模块对登录用户进行身份标识和鉴别；

b） 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

c） 应提供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；

d） 应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

e） 应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。

3.4.2 访问控制

本项要求包括：

a) 应提供访问控制功能，依据安全策略控制用户对文件、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，并严格限制默认帐户的访问权限；
d) 应授予不同帐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) 应具有对重要信息资源设置敏感标记的功能；
f) 应依据安全策略严格控制用户对有敏感标记重要信息资源的操作；

3.4.3 安全审计

本项要求包括：

a) 应提供覆盖到每个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、时间、发起者信息、类型、描述和结果等；
d) 应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。
e) 审计设备能够进行统一管理，审计数据能够集中存储。

3.4.4 剩余信息保护

本项要求包括：

a) 应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；
b) 应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

3.4.5 通信完整性

应采用密码技术保证通信过程中数据的完整性。

3.4.6 通信保密性

本项要求包括：

a) 在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；针对移动办公应采用VPDN线路结合SSL VPN设备对传输链路进行加密。
b) 应对通信过程中的整个报文或会话过程进行加密。

3.4.7 抗抵赖

本项要求包括：

a) 应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；
b) 应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。

3.4.8 软件容错

本项要求包括：

c) 应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；
d) 应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。

3.4.9 资源控制

本项要求包括：

a) 当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；
b) 应能够对系统的最大并发会话连接数进行限制；
c) 应能够对单个帐户的多重并发会话进行限制；
d) 应能够对一个时间段内可能的并发会话连接数进行限制；

e） 应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；

f） 应能够对系统服务水平降低到预先规定的最小值进行检测和报警；

g） 应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。

3.5 数据安全及备份恢复

3.5.1 数据完整性

本项要求包括：

a） 应能够检测到系统管理数据、鉴别信息和重要业务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；

b） 应能够检测到系统管理数据、鉴别信息和重要业务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。

3.5.2 数据保密性

本项要求包括：

a） 应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；

b） 应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。

3.5.3 备份和恢复

本项要求包括：

a） 应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；应采用数据备份一体机或者备份软件。

b） 应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；

c） 应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；

d） 应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。

4 管理标准

4.1 安全管理制度

4.1.1 管理制度

本项要求包括：

a） 应制定信息安全工作的总体方针和安全策略，说明机构安全工作的总体目标、范围、原则和安全框架等；
b） 应对安全管理活动中的各类管理内容建立安全管理制度；
c） 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；
d） 应形成由安全策略、管理制度、操作规程等构成的全面的信息安全管理制度体系。

4.1.2 制定和发布

本项要求包括：

a） 应指定或授权专门的部门或人员负责安全管理制度的制定；
b） 安全管理制度应具有统一的格式，并进行版本控制；
c） 应组织相关人员对制定的安全管理制度进行论证和审定；
d） 安全管理制度应通过正式、有效的方式发布；
e） 安全管理制度应注明发布范围，并对收发文进行登记。

4.1.3 评审和修订

本项要求包括：

a) 信息安全领导小组应负责定期组织相关部门和相关人员对安全管理制度体系的合理性和适用性进行审定；
b) 应定期或不定期对安全管理制度进行检查和审定，对存在不足或需要改进的安全管理制度进行修订。

4.2 安全管理机构

4.2.1 岗位设置

本项要求包括：

a) 应设立信息安全管理工作的职能部门，设立安全主管、安全管理各个方面的负责人岗位，并定义各负责人的职责，同时报上一级法院备案；
b) 应设立系统管理员、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) 应成立指导和管理信息安全工作的委员会或领导小组，其最高领导由单位主管领导委任或授权；
d) 应制定文件明确安全管理机构各个部门和岗位的职责、分工和技能要求。

4.2.2 人员配备

本项要求包括：

a) 应配备一定数量的系统管理员、网络管理员、安全管理员等；
b) 应配备具有正式编制的干警为安全管理员，并将其个人信息、联系方式报上一级法院备案，如有人员调整，及时上报；
c) 关键事务岗位应配备多人共同管理。

4.2.3 授权和审批

本项要求包括：

a) 应根据各个部门和岗位的职责明确授权审批事项、审批部门和批准人等；
b) 应针对系统变更、重要操作、物理访问和系统接入等事项建立审批程序，按照审批程序执行审批过程，对重要活动建立逐级审批制度；

c） 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息；

d） 应记录审批过程并保存审批文档。

4.2.4 沟通和合作

本项要求包括：

a） 应加强各类管理人员之间、组织内部机构之间以及信息安全职能部门内部的合作与沟通，定期或不定期召开协调会议，共同协作处理信息安全问题；

b） 应加强与兄弟单位、公安机关、电信公司的合作与沟通；

c） 应加强与供应商、业界专家、专业的安全公司、安全组织的合作与沟通；

d） 应建立外联单位联系列表，包括外联单位名称、合作内容、联系人和联系方式等信息；

e） 应聘请信息安全专家作为常年的安全顾问，指导信息安全建设，参与安全规划和安全评审等。

4.2.5 审核和检查

本项要求包括：

a） 安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

b） 应由内部人员或上级单位定期进行全面安全检查，检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等；

c） 应制定安全检查表格实施安全检查，汇总安全检查数据，形成安全检查报告，并对安全检查结果进行通报；

d） 应制定安全审核和安全检查制度规范安全审核和安全检查工作，定期按照程序进行安全审核和安全检查活动。

4.3 人员安全管理

4.3.1 人员录用

本项要求包括：

a） 应指定或授权专门的部门或人员负责人员录用；

b） 应严格规范人员录用过程，对被录用人的身份、背景、专业资格和资质等进行审查，对其所具有的技术技能进行考核；

c） 应签署保密协议；

d） 应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议。

4.3.2 人员离岗

本项要求包括：

a） 应严格规范人员离岗过程，及时终止离岗员工的所有访问权限；

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；

c） 应办理严格的调离手续，关键岗位人员离岗须承诺调离后的保密义务后方可离开。

4.3.3 人员考核

本项要求包括：

a） 应定期对各个岗位的人员进行安全技能及安全认知的考核；

b） 应对关键岗位的人员进行全面、严格的安全审查和技能考核；

c） 应对考核结果进行记录并保存。

4.3.4 安全意识教育培训

本项要求包括：

a） 应对各类人员进行安全意识教育、岗位技能培训和相关安全技术培训；

b） 应对安全责任和惩戒措施进行书面规定并告知相关人员，对违反违背安全策略和规定的人员进行惩戒；

c） 应对定期安全教育和培训进行书面规定，针对不同岗位制定不同的培训计划，对信息安全基础知识、岗位操作规程等进行培训；

d） 应对安全教育和培训的情况和结果进行记录并归档保存。

4.3.5 外部人员访问管理

本项要求包括：

a） 应确保在外部人员访问受控区域前先提出书面申请，批准后由专人全程陪同或监督，并登记备案；
b） 对外部人员允许访问的区域、系统、设备、信息等内容应进行书面的规定，并按照规定执行。

4.4 系统建设管理

4.4.1 系统定级

本项要求包括：

a） 应明确信息系统的边界和安全保护等级；
b） 应以书面的形式说明确定信息系统为某个安全保护等级的方法和理由；
c） 应组织相关部门和有关安全技术专家对信息系统定级结果的合理性和正确性进行论证和审定；
d） 应确保信息系统的定级结果经过相关部门的批准。

4.4.2 安全方案设计

本项要求包括：

a） 应根据系统的安全保护等级选择基本安全措施，并依据风险分析的结果补充和调整安全措施；
b） 应指定和授权专门的部门对信息系统的安全建设进行总体规划，制定近期和远期的安全建设工作计划；
c） 应根据信息系统的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件；

d） 应组织相关部门和有关安全技术专家对总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件的合理性和正确性进行论证和审定，并且经过批准后，才能正式实施；

e） 应根据等级测评、安全评估的结果定期调整和修订总体安全策略、安全技术框架、安全管理策略、总体建设规划、详细设计方案等相关配套文件。

4.4.3 产品采购和使用

本项要求包括：

a） 应确保安全产品采购和使用符合国家的有关规定；

b） 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；

c） 应指定或授权专门的部门负责产品的采购；

d） 应预先对产品进行选型测试，确定产品的候选范围，并定期审定和更新候选产品名单。

4.4.4 自行软件开发

本项要求包括：

a） 应确保开发环境与实际运行环境物理分开，开发人员和测试人员分离，测试数据和测试结果受到控制；

b） 应制定软件开发管理制度，明确说明开发过程的控制方法和人员行为准则；

c） 应制定代码编写安全规范，要求开发人员参照规范编写代码；

d） 应确保提供软件设计的相关文档和使用指南，并由专人负责保管；

e） 应确保对程序资源库的修改、更新、发布进行授权和批准。

4.4.5 外包软件开发

本项要求包括：

a） 应根据开发需求检测软件质量；

b） 应在软件安装之前检测软件包中可能存在的恶意代码；

c） 应要求开发单位提供软件设计的相关文档和使用指南；

d） 应要求开发单位提供软件源代码，并审查软件中可能存在的后门。

4.4.6 工程实施

本项要求包括：

a） 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；

b） 应制定详细的工程实施方案控制实施过程，并要求工程实施单位能正式地执行安全工程过程；

c） 应制定工程实施方面的管理制度，明确说明实施过程的控制方法和人员行为准则。

4.4.7 测试验收

本项要求包括：

a） 应委托公正的第三方测试单位对系统进行安全性测试，并出具安全性测试报告；

b） 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，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告；

c） 应对系统测试验收的控制方法和人员行为准则进行书面规定；

d） 应指定或授权专门的部门负责系统测试验收的管理，并按照管理规定的要求完成系统测试验收工作；

e） 应组织相关部门和相关人员对系统测试验收报告进行审定，并签字确认。

4.4.8 系统交付

本项要求包括：

a） 应制定详细的系统交付清单，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；

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；

d） 应对系统交付的控制方法和人员行为准则进行书面规定；

e） 应指定或授权专门的部门负责系统交付的管理工作，并按照管理规定的要求完成系统交付工作。

4.4.9 系统备案

本项要求包括：

a） 应指定专门的部门或人员负责管理系统定级的相关材料，并控制这些材料的使用；
b） 应将系统等级及相关材料报系统主管部门备案；
c） 应将系统等级及其他要求的备案材料报相应公安机关备案。

4.4.10 等级测评

本项要求包括：

a） 在系统运行过程中，应至少每年对系统进行一次等级测评，发现不符合相应等级保护标准要求的及时整改；
b） 应在系统发生变更时及时对系统进行等级测评，发现级别发生变化的及时调整级别并进行安全改造，发现不符合相应等级保护标准要求的及时整改；
c） 应选择具有国家相关技术资质和安全资质的测评单位进行等级测评；
d） 应指定或授权专门的部门或人员负责等级测评的管理。

4.4.11 安全服务商选择

本项要求包括：

a） 应确保安全服务商的选择符合国家的有关规定；
b） 应与选定的安全服务商签订与安全相关的协议，明确约定相关责任；
c） 应确保选定的安全服务商提供技术培训和服务承诺，必要的与其签订服务合同。

4.5 系统运维管理

4.5.1 环境管理

本项要求包括：

a) 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管理；
b) 应指定部门负责机房安全，并配备机房安全管理人员，对机房的出入、服务器的开机或关机等工作进行管理；
c) 应建立机房安全管理制度，对有关机房物理访问，物品带进、带出机房和机房环境安全等方面的管理作出规定；
d) 应加强对办公环境的保密性管理，规范办公环境人员行为，包括工作人员调离办公室应立即交还该办公室钥匙、不在办公区接待来访人员、工作人员离开座位应确保终端计算机退出登录状态和桌面上没有包含敏感信息的纸档文件等。

4.5.2 资产管理

本项要求包括：

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) 应建立资产安全管理制度，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；
c) 应根据资产的重要程度对资产进行标识管理，根据资产的价值选择相应的管理措施；
d) 应对信息分类与标识方法作出规定，并对信息的使用、传输和存储等进行规范化管理。

4.5.3 介质管理

本项要求包括：

a) 应建立介质安全管理制度，对介质的存放环境、使用、维护和销毁等方面作出规定；

b) 应确保介质存放在安全的环境中，对各类介质进行控制和保护，并实行存储环境专人管理；

c) 应对介质在物理传输过程中的人员选择、打包、交付等情况进行控制，对介质归档和查询等进行登记记录，并根据存档介质的目录清单定期盘点；

d) 应对存储介质的使用过程、送出维修以及销毁等进行严格的管理，对带出工作环境的存储介质进行内容加密和监控管理，对送出维修或销毁的介质应首先清除介质中的敏感数据，对保密性较高的存储介质未经批准不得自行销毁；

e) 应根据数据备份的需要对某些介质实行异地存储，存储地的环境要求和管理方法应与本地相同；

f) 应对重要介质中的数据和软件采取加密存储，并根据所承载数据和软件的重要程度对介质进行分类和标识管理。

4.5.4 设备管理

本项要求包括：

a) 应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门的部门或人员定期进行维护管理；

b) 应建立基于申报、审批和专人负责的设备安全管理制度，对信息系统的各种软硬件设备的选型、采购、发放和领用等过程进行规范化管理；

c) 应建立配套设施、软硬件维护方面的管理制度，对其维护进行有效的管理，包括明确维护人员的责任、涉外维修和服务的审批、维修过程的监督控制等；

d) 应对终端计算机、工作站、便携机、系统和网络等设备的操作和使用进行规范化管理，按操作规程实现主要设备（包括备份和冗余设备）的启动/停止、加电/断电等操作；

e) 应确保信息处理设备必须经过审批才能带离机房或办公地点。

4.5.5 监控管理和安全管理中心

本项要求包括：

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、用户行为等进行监测和报警，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，发现可疑行为，形成分析报告，并采取必要的应对措施；
c） 应建立安全管理中心，对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行集中管理。

4.5.6 网络安全管理

本项要求包括：

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；
e） 应实现设备的最小服务配置，并对配置文件进行定期离线备份；
f） 应保证所有与外部系统的连接均得到授权和批准；
g） 应依据安全策略允许或者拒绝便携式和移动式设备的网络接入；
h） 应定期检查违反规定拨号上网或其他违反网络安全策略的行为。

4.5.7 系统安全管理

本项要求包括：

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） 应指定专人对系统进行管理，划分系统管理员角色，明确各个角色的权限、责任和风险，权限设定应当遵循最小授权原则；

f） 应依据操作手册对系统进行维护，详细记录操作日志，包括重要的日常操作、运行维护记录、参数的设置和修改等内容，严禁进行未经授权的操作；

g） 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。

4.5.8 恶意代码防范管理

本项要求包括：

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） 应对防恶意代码软件的授权使用、恶意代码库升级、定期汇报等作出明确规定；

d） 应定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，对主机防病毒产品、防病毒网关和邮件防病毒网关上截获的危险病毒或恶意代码进行及时分析处理，并形成书面的报表和总结汇报。

4.5.9 密码管理

应建立密码使用管理制度，使用符合国家密码管理规定的密码技术和产品。

4.5.10 变更管理

本项要求包括：

a） 应确认系统中要发生的变更，并制定变更方案；

b） 应建立变更管理制度，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） 应建立变更控制的申报和审批文件化程序，对变更影响进行分析并文档化，记录变更实施过程，并妥善保存所有文档和记录；

d） 应建立中止变更并从失败变更中恢复的文件化程序，明确过程控制方法和人员职责，必要时对恢复过程进行演练。

4.5.11 备份与恢复管理

本项要求包括：

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安全管理制度，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；

d） 应建立控制数据备份和恢复过程的程序，对备份过程进行记录，所有文件和记录应妥善保存；

e） 应定期执行恢复程序，检查和测试备份介质的有效性，确保可以在恢复程序规定的时间内完成备份的恢复。

4.5.12 安全事件处置

本项要求包括：

a） 应报告所发现的安全弱点和可疑事件，但任何情况下用户均不应尝试验证弱点；

b） 应制定安全事件报告和处置管理制度，明确安全事件的类型，规定安全事件的现场处理、事件报告和后期恢复的管理职责；

c） 应根据国家相关管理部门对计算机安全事件等级划分方法和安全事件对本系统产生的影响，对本系统计算机安全事件进行等级划分；

d） 应制定安全事件报告和响应处理程序，确定事件的报告流程，响应和处置的范围、程度，以及处理方法等；

e） 应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据，记录处理过程，总结经验教训，制定防止再次发生的补救措施，过程形成的所有文件和记录均应妥善保存；

f） 对造成系统中断和造成信息泄密的安全事件应采用不同的处理程序和报告程序。

4.5.13 应急预案管理

本项要求包括：

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） 应从人力、设备、技术和财务等方面确保应急预案的执行有足够的资源保障；

c） 应对系统相关的人员进行应急预案培训，应急预案的培训应至少每年举办一次；

d） 应定期对应急预案进行演练，根据不同的应急恢复内容，确定演练的周期；

e） 应规定应急预案需要定期审查和根据实际情况更新的内容，并按照执行。