ICS 35.040
CCS L 80

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T XXX—XXXX

多功能智能杆　信息系统安全管理规范

Multifunctional smart pole—Security management requirements for information system

（送审稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 实施

深圳市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件由深圳市工业和信息化局提出并归口。

本文件起草单位：深圳市脉山龙信息技术股份有限公司、深圳市洲明科技股份有限公司、深圳市信息基础设施投资发展有限公司、北京天融信网络安全技术有限公司、金砖国家未来网络研究院(中国·深圳)、深圳大学、深圳市震有智联科技有限公司、信安软件测评认证中心（深圳）有限公司。

本文件主要起草人：李海燕、陈铎航、王玉、林奕康、陈政浩、汪书福、林洺锋、陈晓宁、张帆、黄永衡、许亚萍、陈挺、江魁、刘向华、王先峰、张金钟、马龙彪、宋建民、陈希、张勇、白莹杰、杨彪。

多功能智能杆　信息系统安全管理规范

1　范围

本文件规定了多功能智能杆信息系统安全管理的内容、原则、策略、制度、机构建设、人员管理、风险管理和控制、运维和服务管理。

本文件适用于指导多功能智能杆信息系统安全管理工作，涉密多功能智能杆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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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 20271—2006　信息安全技术　信息系统通用安全技术要求

GB/T 25069—2022　信息安全技术　术语

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 50016—2014　建筑设计防火规范

3　术语和定义

GB/T 25069—2022和GB/T 37095—2018界定的以及下列术语和定义适用于本文件。

3.1

完整性 integrity

数据、系统或信息在存储、传输和处理过程中保持无误、不受损坏、不受篡改的状态，包括数据完整性和系统完整性。

注1：数据完整性：数据在存储、传输和处理过程中保持准确、完整和可信的状态。

注2：系统完整性：系统在非授权用户修改或使用资源和授权用户不正确地修改或使用资源的情况下，保持其正常可靠运行的状态。

3.2

可用性　availability

表征数据或系统根据授权实体的请求可被访问与使用程度的属性。

3.3

访问控制　access control

按确定的规则防止对资源的未授权使用，对实体之间的访问活动进行控制的安全机制。

3.4

安全审计　security audit

按确定规则的要求，对与安全相关的事件进行审计，以日志方式记录必要信息，并作出相应处理的安全机制。

3.5

鉴别信息 authentication information

用以确认系统中身份真实性的过程。

3.6

风险评估 risk assessment

通过对信息系统的资产价值/重要性、信息系统所受到的威胁以及信息系统的脆弱性进行综合分析，对信息系统及其处理、传输和存储的信息的保密性、完整性和可用性等进行科学识别和评价，确定信息 系统安全风险的过程。

3.7

安全策略 security policy

为信息系统安全管理制定的行动方针、路线、工作方式、指导原则或程序。

4 信息系统安全管理

4.1 信息系统安全管理内容

多功能智能杆信息系统安全管理是对管理平台、移动互联、挂载设备和公共数据的生存周期全过程实施符合安全等级责任要求的管理，包括但不限于以下内容：

a) 落实安全管理机构及安全管理人员，明确角色与职责，制定安全规划；
b) 开发安全策略；
c) 实施风险管理；
d) 制定业务持续性计划和灾难恢复计划；
e) 选择与实施安全措施；
f) 保证配置、变更的正确与安全；
g) 进行安全审计；
h) 保证维护支持；
i) 进行监控、检查，处理安全事件；
j) 安全意识与安全教育；
k) 人员安全管理等。

4.2 信息系统安全管理原则

4.2.1 基于安全需求原则

组织机构应根据其信息系统担负的使命，积累的信息资产的重要性，可能受到的威胁及面临的风险分析安全需求，按照信息系统等级保护要求确定相应的信息系统安全保护等级，遵从相应等级的规范要求，从全局上恰当地平衡安全投入与效果。

4.2.2 主要领导负责原则

主要领导应确立其组织统一的信息安全保障的宗旨和政策，负责提高员工的安全意识，组织有效安全保障队伍，调动并优化配置必要的资源，协调安全管理工作与各部门工作的关系，并确保其落实、有效。

4.2.3 全员参与原则

信息系统所有相关人员应普遍参与信息系统的安全管理，并与相关方面协同、协调，共同保障信息系统安全。

4.2.4 系统方法原则

按照系统工程的要求，识别和理解信息安全保障相互关联的层面和过程，采用管理和技术结合的方法，提高实现安全保障的目标的有效性和效率。

4.2.5 持续改进原则

安全管理是一种动态反馈过程，贯穿整个安全管理的生存周期，随着安全需求和系统脆弱性的时空分布变化，威胁程度的提高，系统环境的变化以及对系统安全认识的深化等，应及时地将现有的安全策略、风险接受程度和保护措施进行复查、修改、调整以至提升安全管理等级，维护和持续改进信息安全管理体系的有效性。

4.2.6 依法管理原则

信息安全管理工作主要体现为管理行为，应保证信息系统安全管理主体合法、管理行为合法、管理内容合法、管理程序合法。对安全事件的处理，应由授权者适时发布准确一致的有关信息，避免带来不良的社会影响。

4.2.7 分权和授权原则

对特定职能或责任领域的管理功能实施分离、准入审批、独立审计等实行分权，避免权力过分集中所带来的隐患，以减小未授权的修改或滥用系统资源的机会。任何实体（如用户、管理员、进程、应用或系统）仅享有该实体需要完成其任务所必须的权限，不应享有任何多余权限。

4.2.8 选用成熟技术原则

成熟的技术具有较好的可靠性和稳定性，采用新技术时要重视其成熟的程度，并应首先局部试点然后逐步推广，以减少或避免可能出现的失误。

4.2.9 分级保护原则

按等级划分标准确定信息系统的安全保护等级，实行分级保护；对多个子系统构成的大型信息系统，确定系统的基本安全保护等级，并根据实际安全需求，分别确定各子系统的安全保护等级，实行多级安全保护。

4.2.10 管理与技术并重原则

坚持积极防御和综合防范，全面提高信息系统安全防护能力，立足国情，采用管理与技术相结合，管理科学性和技术前瞻性结合的方法，保障信息系统的安全性达到所要求的目标。

4.2.11 自保护和国家监管结合原则

对信息系统安全实行自保护和国家保护相结合。组织机构要对自己的信息系统安全保护负责，政府相关部门有责任对信息系统的安全进行指导、监督和检查，形成自管、自查、自评和国家监管相结合的管理模式，提高信息系统的安全保护能力和水平，保障国家信息安全。

4.3 信息系统安全管理策略

4.3.1 基本的安全管理策略

应制定信息系统安全管理工作的总体方针和安全策略，阐明机构安全工作的总体目标、范围、原则和安全框架等。

信息系统安全管理策略包括：依照国家政策法规和技术及管理标准进行自主保护；阐明管理者对信息系统安全的承诺，并陈述组织机构管理信息系统安全的方法；说明信息系统安全的总体目标、范围和安全框架；申明支持信息系统安全目标和原则的管理意向；简要说明对组织机构有重大意义的安全方针、原则、标准和符合性要求。

4.3.2 完整的安全管理策略

在基本的安全管理策略的基础上，完整的信息安全管理策略还包括：在信息安系统全监管职能部门的指导下，依照国家政策法规和技术及管理标准自主进行保护；明确划分信息系统（分系统/域）的安全保护等级（按区域分等级保护）；制定风险管理策略、业务连续性策略、安全培训与教育策略、审计策略等较完整的信息安全策略。

4.3.3 体系化的安全管理策略

在完整的安全管理策略的基础上，体系化的信息安全管理策略还包括：在接受信息系统安全监管职能部门监督、检查的前提下，依照国家政策法规和技术及管理标准自主进行保护；制定目标策略、规划策略、机构策略、人员策略、管理策略、安全技术策略、控制策略、生存周期策略、投资策略、质量策略等，形成体系化的信息系统安全策略。

4.3.4 强制保护的安全管理策略

在体系化的安全管理策略的基础上，强制保护的信息安全管理策略还包括：在接受信息系统安全监管职能部门的强制监督、检查的前提下，依照国家政策法规和技术及管理标准自主进行保护；制定体系完整的信息系统安全管理策略。

4.3.5 专控保护的安全管理策略

在强制保护的安全管理策略的基础上，专控保护的信息安全管理策略还包括：在接受国家指定的专门部门、专门机构的专门监督的前提下，依照国家政策法规和技术及管理标准自主进行保护；制定可持续改进的信息系统安全管理策略。

4.4 信息系统安全管理制度

4.4.1 基本的安全管理制度

应对多功能智能杆的管理平台、移动互联、挂载设备和公共数据安全管理活动中的各类管理内容建立安全管理制度；从安全组织、安全责任、访问控制、系统设计、系统建设、系统验收、系统运维、应急处置、人员管理、文件档案管理、审核检查等方面规范各项网络安全管理工作。

4.4.2 完整的安全管理制度

在基本的安全管理制度的基础上，应增加人员安全管理规定、安全审计管理规定、用户管理规定、风险管理规定、信息分类分级管理规定、安全事件报告规定、事故处理规定、应急管理规定和灾难恢复管理规定等制度。

4.4.3 体系化的安全管理制度

4.4.3.1 应制定安全管理规定，包括：机房、主机设备、网络设施、物理设施分类标记等系统资源安全管理规定。

4.4.3.2 应制定安全配置、系统分发和操作、系统文档、测试和脆弱性评估、系统信息安全备份和相关的操作规程等系统和数据库方面的安全管理规定。

4.4.3.3 应制定系统互联评估、网络使用授权、网络检测、网络设施（设备和协议）变更控制和相关的操作规程等方面的网络安全管理规定。

4.4.3.4 应制定系统安全评估、应用系统使用授权、应用系统配置管理、应用系统文档管理和相关的操作规程等方面的应用安全管理规定。

4.4.3.5 应制定人员安全管理、安全意识与安全技术教育、操作安全、操作系统和数据库安全、系统运行记录、病毒防护、系统维护、网络互联、安全审计、安全事件报告、事故处理、应急管理、灾难恢复和相关的操作规程等方面的运行安全管理规定。

4.4.3.6 应制定信息分类标记、涉密信息管理、文档管理、存储介质管理、信息披露与发布审批管理、第三方访问控制和相关的操作规程等方面的信息安全管理规定。

4.4.4 强制保护的安全管理制度

在体系化的安全管理制度的基础上，应制定信息保密标识与管理规定、密码使用管理规定、安全事件例行评估和报告规定、关键控制措施定期测试规定等制度。

4.4.5 专控保护的安全管理制度

在强制保护的安全管理制度的基础上，应制定安全管理审计监督规定等制度。

5 机构建设和人员管理

5.1 建立安全管理机构

不同安全等级建立的安全管理机构，有选择地满足以下要求的一项：

a) 配备安全管理人员：管理层中应有一人分管信息系统安全工作，并为信息系统的安全管理配备专职或兼职的安全管理人员；

b) 建立安全职能部门：在 a）的基础上，应建立管理信息系统安全工作的职能部门，或者明确指定一个职能部门兼管信息安全工作，作为该部门的关键职责之一；

c) 成立安全领导小组：在 b）的基础上，应在管理层成立信息系统安全管理委员会或信息系统安全领导小组，对覆盖全国或跨地区的组织机构，应在总部和下级单位建立各级信息系统安全领导小组，在基层至少要有一位专职的安全管理人员负责信息系统安全工作；

d) 主要负责人出任领导：在 c）的基础上，应由组织机构的主要负责人出任信息系统安全领导小组负责人；

e) 建立信息安全保密管理部门：在 d）的基础上，应建立信息系统安全保密监督管理的职能部门，或对原有保密部门明确信息安全保密管理责任，加强对信息系统安全管理重要过程和管理人员的保密监督管理。

5.2 信息安全领导小组

信息系统安全领导小组负责领导本组织机构的信息系统安全工作，至少行使以下管理职能之一:

a) 安全管理的领导职能：根据国家和行业有关信息安全的政策、法律和法规，批准机构信息系统的安全策略和发展规划；确定各有关部门在信息系统安全工作中的职责，领导安全工作的实施；监督安全措施的执行，并对重要安全事件的处理进行决策；指导和检查信息系统安全职能部门及应急处理小组的各项工作；建设和完善信息系统安全的集中控管的组织体系和管理机制；
b) 保密监督的管理职能：在 a）的基础上，对保密管理部门进行有关信息系统安全保密监督管理方面的指导和检查。

5.3 信息安全职能部门

信息安全职能部门在信息系统安全领导小组领导下，负责本组织机构信息系统安全的具体工作，至少应行使以下管理职能之一：

a) 基本的安全管理职能：根据国家和行业有关信息安全的政策法规，起草组织机构信息系统的安全策略和发展规划；管理机构信息系统安全日常事务，检查和指导下级单位信息系统安全工作；负责安全措施的实施或组织实施，组织并参加对安全重要事件的处理；监控信息系统安全总体状况，提出安全分析报告；指导和检查各部门和下级单位信息系统安全人员及要害岗位人员的信息系统安全工作；应与有关部门共同组成应急处理小组或协助有关部门建立应急处理小组实施相关应急处理工作；
b) 集中的安全管理职能：在基本的安全管理职能的基础上，管理信息系统安全机制集中管理机构的各项工作，实现信息系统安全的集中控制管理；完成信息系统安全领导小组交办的工作，并向领导小组报告机构的信息系统安全工作。

5.4 安全管理人员配备

不同安全等级的安全管理人员配备，有选择地满足以下要求的一项：

a) 可配备兼职安全管理人员：安全管理人员可以由网络管理人员兼任；
b) 安全管理人员的兼职限制：安全管理人员不能兼任网络管理人员、系统管理员、数据库管理员等；
c) 配备专职安全管理人员：安全管理人员不可兼任，属于专职人员，应具有安全管理工作权限和能力；
d) 关键部位的安全管理人员：在 c）的基础上，安全管理人员还应按照机要人员条件配备。

5.5 关键岗位人员管理

不同安全等级的关键岗位人员管理，可有选择地满足以下要求的一项或多项：

a) 基本要求：应对安全管理员、系统管理员、数据库管理员、网络管理员、重要业务开发人员、系统维护人员、重要业务应用操作人员等信息系统关键岗位人员进行统一管理；允许一人多岗，但业务应用操作人员不能由其他关键岗位人员兼任；关键岗位人员应定期接受安全培训，加强安全意识和风险防范意识；
b) 兼职和轮岗要求：业务开发人员和系统维护人员不能兼任或担负安全管理员、系统管理员、数据库管理员、网络管理员、重要业务应用操作人员等岗位或工作；必要时关键岗位人员应采取定期轮岗制度；
c) 权限分散要求：在 b）的基础上，应坚持关键岗位人员“权限分散、不应交叉覆盖”的原则，系统管理员、数据库管理员、网络管理员不能相互兼任岗位或工作；
d) 多人共管要求：在 c）的基础上，关键岗位人员处理重要事务或操作时，应保持二人同时在场，关键事务应多人共管；
e) 全面控制要求：在 d）的基础上，应采取对内部人员全面控制的安全保证措施，对所有岗位工作人员实施全面安全管理。

5.6 人员录用管理

不同安全等级的人员录用管理，可有选择地满足以下要求的一项：

a) 人员录用的基本要求：对应聘者进行审查，确认其具有基本的专业技术水平，接受过安全意识教育和培训，能够掌握安全管理基本知识；对信息系统关键岗位的人员还应注重思想品质方面的考察；
b) 人员的审查与考核：在 a）的基础上，应由单位人事部门进行人员背景、资质审查，技能考核等，合格者还要签署保密协议方可上岗；安全管理人员应具有基本的系统安全风险分析和评估能力；
c) 人员的内部选拔：在 b）的基础上，重要区域或部位的安全管理人员一般可从内部符合条件人员选拔，应做到认真负责和保守秘密；
d) 人员的可靠性：在 c）的基础上，关键区域或部位的安全管理人员应选用实践证明精干、内行、忠实、可靠的人员，必要时可按机要人员条件配备。

5.7 人员离岗管理

不同安全等级对人员离岗的管理，有选择地满足以下要求的一项：

a) 离岗的基本要求：立即中止被解雇的、退休的、辞职的或其他原因离开的人员的所有访问权限；收回所有相关证件、徽章、密钥、访问控制标记等；收回机构提供的设备等；
b) 调离后的保密要求：在 a）的基础上，管理层和信息系统关键岗位人员调离岗位，应经单位人事部门严格办理调离手续，承诺其调离后的保密要求；
c) 离岗的审计要求：在 b）的基础上，涉及组织机构管理层和信息系统关键岗位的人员调离单位，必须进行离岗安全审查，在规定的脱密期限后，方可调离；
d) 关键部位人员的离岗要求：在 c）的基础上，关键部位的信息系统安全管理人员离岗，应按照机要人员管理办法办理。

5.8 人员考核与审查

不同安全等级的人员考核与审查管理，有选择地满足以下要求的一项：

a) 定期的人员考核：应定期对各个岗位的人员进行不同侧重的安全认知和安全技能的考核，作为人员是否适合当前岗位的参考；
b) 定期的人员审查：在人员考核的基础上，对关键岗位人员，应定期进行审查，如发现其违反安全规定，应控制使用；
c) 管理有效性的审查：在定期人员审查的基础上，对关键岗位人员的工作，应通过例行考核进行审查，保证安全管理的有效性；并保留审查结果；
d) 全面严格的审查：在有效性审查的基础上，对所有安全岗位人员的工作，应通过全面考核进行审查，如发现其违反安全规定，应采取必要的应对措施。

5.9 人员教育和培训

不同安全等级的人员教育和培训，有选择地满足以下要求的一项：
a) 应知应会要求培训：应让信息系统相关员工知晓信息的敏感性和信息安全的重要性，认识其自身的责任和安全违例会受到纪律惩罚，以及应掌握的信息安全基本知识和技能等；
b) 有计划培训：在应知应会要求的基础上，应制定并实施安全教育和培训计划，培养信息系统各类人员安全意识，并提供对安全政策和操作规程的认知教育和训练等；
c) 针对不同岗位培训：在计划培训的基础上，针对不同岗位，制定不同的专业培训计划，包括安全知识、安全技术、安全标准、安全要求、法律责任和业务控制措施等；
d) 按人员资质要求培训：在岗位培训的基础上，对所有工作人员的安全资质进行定期检查和评估，使相应的安全教育成为组织机构工作计划的一部分；
e) 安全意识自觉性培训：在资质培训的基础上，对所有工作人员进行相应的安全资质管理，并使安全意识成为所有工作人员的自觉行动。

6 风险管理和控制

6.1 风险管理要求

风险管理作为等级保护的手段，在保证信息等级系统的最低保护能力的基础上，可根据风险确定增加某些管理要求。

不同安全等级的风险管理，有选择地满足以下要求的一项：
a) 基本风险管理：组织机构应进行基本的风险管理活动，包括编制资产清单，对资产价值/重要性进行分析，对信息系统面临的威胁进行初步分析，通过工具扫描的方式对信息系统的脆弱性进行分析，以简易的方式分析安全风险、选择安全措施；
b) 定期风险评估：在基本风险管理的基础上，针对关键的系统资源进行定期风险分析和评估；产生风险分析报告并向管理层提交；
c) 规范风险评估：在定期风险评估的基础上，在风险管理中，使用规范方法和经过必要的工作流程，进行规范化的风险评估，产生风险分析报告和留存重要过程文档，并向管理层提交；
d) 独立审计的风险管理：在规范风险评估的基础上，建立风险管理体系文件；针对风险管理过程，实施独立审计，确保风险管理的有效性；
e) 全面风险管理：在独立审计风险管理的基础上，使风险管理成为信息系统安全管理的有机组成部分，贯穿信息系统安全管理的全过程，并具有可验证性。

6.2 风险管理策略

不同安全等级的风险管理策略，有选择地满足以下要求的一项：

a) 基本的风险管理策略：应定期进行风险评估，安全风险分析和评估活动程序应至少包括信息安全风险管理和业务应用风险管理密切相关的内容，信息安全风险管理的基本观念和方法，以及风险管理的组织和资源保证等；
b) 风险管理的监督机制：在基本的风险管理策略的基础上，应建立风险管理的监督机制，对所有风险管理相关过程的活动和影响进行评估和监控；应建立指导风险管理监督过程的指导性文档；
c) 风险评估的重新启动：在风险管理监督机制的基础上，应明确规定重新启动风险评估的条件，机构应能针对风险的变化重新启动风险评估。

6.3 风险分析

6.3.1 资产识别和分析

不同安全等级的资产识别和分析，有选择地满足以下要求的一项：

a) 信息系统的资产统计和分类：确定信息系统的资产范围，进行统计和编制资产清单（详见 7.2.1），并进行资产分类和重要性标识；
b) 信息系统的体系特征描述：在资产统计和分类的基础上，根据对信息系统的硬件、软件、系统接口、数据和信息、人员等方面的分析和识别，对信息系统的体系特征进行描述，至少应阐明信息系统的使命、边界、功能，以及系统和数据的关键性、敏感性等内容。

6.3.2 威胁识别和分析

不同安全等级的威胁识别和分析，有选择地满足以下要求的一项：

a) 威胁的基本分析：应根据以往发生的安全事件、外部提供的资料和积累的经验等，对威胁进行粗略的分析；
b) 威胁的列表分析：在基本分析的基础上，结合业务应用、系统结构特点以及访问流程等因素，建立并维护威胁列表；由于不同业务系统面临的威胁是不同的，应针对每个或者每类资产有一个威胁列表；
c) 威胁的详细分析：在列表分析的基础上，考虑威胁源在保密性、完整性或可用性等方面造成损害，对威胁的可能性和影响等属性进行分析，从而得到威胁的等级；威胁等级也可通过综合威胁的可能性和强度的评价获得；
d) 使用检测工具捕捉攻击：在基本分析详细的基础上，对关键区域或部位进行威胁分析和评估，在业务应用许可并得到批准的条件下，可使用检测工具在特定时间捕捉攻击信息进行威胁分析。

6.3.3 脆弱性识别和分析

不同安全等级的脆弱性识别和分析，有选择地满足以下要求的一项：

a) 脆弱性工具扫描：应通过扫描器等工具来获得对系统脆弱性的认识，包括对管理平台、网络设备、主机设备、挂载设备和安全设备的脆弱性扫描，并编制脆弱性列表，作为

系统加固、改进和安全项目建设的依据；可以针对资产组合、资产分类编制脆弱性列表和脆弱性检查表；

b) 脆弱性分析和渗透测试：在扫描的基础上，脆弱性的分析应使用渗透测试分别从管理平台、网络设备、主机设备、挂载设备、安全设备选择不同的接入点进行；应了解测试可能带来的后果，并做好充分准备；针对不同的资产和资产组合，综合应用人工评估、工具扫描、渗透性测试等方法对系统的脆弱性进行分析和评估；对不同的方法和工具所得出的评估结果，应进行综合分析，从而得到脆弱性的等级；

c) 制度化脆弱性评估：在渗透测试的基础上，坚持制度化脆弱性评估，应明确规定进行脆弱性评估的时间和系统范围、人员和责任、评估结果的分析和报告程序，以及报告中包括新发现的漏洞、已修补的漏洞、漏洞趋势分析等。

6.4 风险评估

不同安全等级的风险评估，有选择地满足以下要求的一项：

a) 经验的风险评估：应由用户和部分专家通过经验来判断风险，并对风险进行评估，形成风险评估报告，其中必须包括风险级别、风险点等内容，并确定信息系统的安全风险状况；

b) 全面的风险评估：在经验风险评估的基础上，应采用多层面、多角度的系统分析方法，由用户和专家对资产、威胁和脆弱性等方面进行定性综合评估，建议处理和减缓风险的措施，形成风险评估报告；除风险状况外，在风险评估的各项步骤中还应生成信息系统体系特征报告、威胁评估报告、脆弱性评估报告和安全措施分析报告等；基于这些报告，评估者应对安全措施提出建议；

c) 建立和维护风险信息库：在全面风险评估的基础上，应将风险评估中的信息资产、威胁、脆弱性、防护措施等评估项信息综合到一个数据库中进行管理；组织机构应当在后续的项目和工具中持续地维护该数据库。

6.5 风险控制

不同安全等级的风险控制，有选择地满足以下要求的一项：

a) 基于安全等级标准选择控制措施：以信息系统及产品的安全等级标准对不同等级的技术和管理要求，选择相应等级的安全技术和管理措施，决定需要实施的信息系统安全控制措施；

b) 基于风险评估选择控制措施：在 a）项的基础上，根据风险评估的结果，结合组织机构对于信息系统安全的需求，决定信息系统安全的控制措施；

c) 基于风险评估形成防护控制系统：在 b）项的基础上，根据风险评估的结果，结合机构对于信息系统安全的需求，决定信息系统安全的控制措施；对相关的各种控制措施进行综合分析，得出紧迫性、优先级、投资比重等评价，形成体系化的防护控制系统。

6.6 安全确认

不同安全等级的安全确认，有选择地满足a+b或者a+c其中两项：

a) 残余风险接受：针对信息系统的资产清单、威胁列表、脆弱性列表，结合已采用的安全控制措施，分析存在的残余风险；应形成残余风险分析报告，并由组织机构的高层管理人员决定残余风险是否可接受；

b） 残余风险监视：在 a）的基础上，应编制出信息系统残余风险清单，并密切监视残余风险可能诱发的安全事件，并及时采取防护措施；
c） 安全风险再评估：在 b）的基础上，采用系统化的方法对信息系统安全风险实施再次评估，通过再次评估，验证防护措施的有效性。

7 运维和服务管理

7.1 物理环境管理

7.1.1 物理环境要求

物理环境要求如下：
a） 物理位置选择：机房场地应选择在具有防震、防风和防雨等能力的建筑内；机房场地应避免设在建筑物的顶层或地下室，否则应加强防水和防潮措施；
b） 防盗窃和防破坏：应将机房设备或主要部件进行固定，并设置明显的不易除去的标识；应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；应设置机房防盗报警系统或设置有专人值守的视频监控系统；
c） 防雷击：应将各类机柜、设施和设备等通过接地系统安全接地；应采取措施防止感应雷，例如设置防雷保安器或过压保护装置等；
d） 防火：应符合 GB 50016—2014 的相关要求；
e） 防水和防潮：应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；应采取措施防止机房内水蒸气结露、水管泄漏和地下积水的转移与渗透；机房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；
f） 防静电：应安装防静电地板或地面并采用必要的接地防静电措施；应采用措施防止静电的产生，例如采用静电消除器、佩戴防静电手环等；
g） 温湿度控制：机房应设置温、湿度自动调节设施；机房的温度范围应在 18° C～26° C 之内，第四级网络所在机房的温度范围应在 19° C～25° C 之内；机房的湿度范围应在 35%～65%之内，第四级网络所在机房的湿度范围应在 40%～60%之内；
h） 电力供应：应在机房供电线路上配置稳压器和过电压防护设备；应提供短期的备用电力供应，至少满足设备在断电情况下的正常运行要求；应设置冗余或并行的电力电缆线路为系统供电；三级及以上网络应接入两路外电，其中至少一路宜为专线，当一路外电发生故障时，另一路外电不应同时受到损害；
i） 电磁防护：电源线和通信线缆应隔离铺设，避免互相干扰；三级及以上网络应对关键设备或关键区域实施电磁屏蔽。

7.1.2 不同安全等级的选择要求

不同安全等级的物理环境安全管理，有选择地满足以下要求的一项：
a） 物理环境安全的基本要求：应配置物理环境安全的责任部门和管理人员；建立有关物理环境安全方面的规章制度；物理安全方面应达到 GB/T 20271—2006 中 6.1.1 的有关要求；
b） 较完整的制度化管理：在 a）的基础上，应对物理环境划分不同保护等级的安全区域进行管理；应制定对物理安全设施进行检验、配置、安装、运行的有关制度和保障措

施；实行关键物理设施的登记制度；物理安全方面应达到 GB/T 20271—2006 中 6.2.1 的有关要求；

c) 安全区域标记管理：在 b）的基础上，应对物理环境中所有安全区域进行标记管理，包括不同安全保护等级的办公区域、机房、介质库房等；介质库房的管理可以参照同等级的机房的要求；物理安全方面应达到 GB/T 20271—2006 中 6.3.1 的有关要求；

d) 安全区域隔离和监视：在 c）的基础上，应实施不同保护等级安全区域的隔离管理；出入人员应经过相应级别的授权并有监控措施；对重要安全区域的活动应实时监视和记录；物理安全方面应达到 GB/T 20271—2006 中 6.4.1 的有关要求；

e) 安全保障的持续改善：在 d）的基础上，应对物理安全保障定期进行监督、检查和不断改进，实现持续改善；物理安全方面应达到 GB/T 20271—2006 中 6.5.1 的有关要求。

7.1.3 机房安全管理要求

不同安全等级的机房安全管理，有选择地满足以下要求的一项：

a) 机房安全管理的基本要求：应明确机房安全管理的责任人，机房出入应有指定人员负责，未经允许的人员不准进入机房；获准进入机房的来访人员，其活动范围应受到限制，并有接待人员陪同；机房钥匙由专人管理，未经批准，不准任何人私自复制机房钥匙或服务器开机钥匙；没有指定管理人员的明确准许，任何记录介质、文件材料及各种被保护品均不准带出机房，与工作无关的物品均不准带入机房；机房内严禁吸烟及带入火种和水源；

b) 加强对来访人员的控制：在 a）的基础上，要求所有来访人员应经过正式批准，登记记录应妥善保存；获准进入机房的来访人员，一般应禁止携带个人计算机等电子设备进入机房，其活动范围和操作行为应受到限制，并有机房接待人员负责和陪同；

c) 增强门禁控制手段：在 b）的基础上，任何进出机房的人员应经过门禁设施的监控和记录，应有防止绕过门禁设施的手段；门禁系统的电子记录应妥善保存以备查；进入机房的人员应佩戴相应证件；未经批准，禁止任何物理访问；未经批准，禁止任何人移动计算机相关设备或带离机房；

d) 使用视频监控和专职警卫：在 c）的基础上，机房所在地应有专职警卫，通道和入口处应设置视频监控点，24 小时值班监视；所有来访人员的登记记录、门禁系统的电子记录以及监视录像记录应妥善保存以备查；禁止携带移动电话、电子记事本等具有移动互连功能的个人物品进入机房；

e) 采取防止电磁泄漏措施：在 d）的基础上，对需要防止电磁泄漏的计算机设备配备电磁干扰设备，在被保护的计算机设备工作时电磁干扰设备不准关机；必要时可以使用屏蔽机房。屏蔽机房应随时关闭屏蔽门；不应在屏蔽墙上随意打孔，不应在波导管以外或不经过过滤器对屏蔽机房内外连接任何线缆；应经常测试屏蔽机房的泄漏情况并进行必要的维护。

7.1.4 办公环境安全管理要求

不同安全等级的办公环境安全管理，有选择地满足以下要求的一项：

a) 办公环境安全管理基本要求：设置有网络终端的办公环境，是信息系统环境的组成部分，应防止利用终端系统窃取敏感信息或非法访问；工作人员下班后，终端计算机应

关闭；存放敏感文件或信息载体的文件柜应上锁或设置密码；工作人员调离部门或更换办公室时，应立即交还办公室钥匙；设立独立的会客接待室，不在办公环境接待来访人员；

b) 办公环境安全管理增强要求：在 a）的基础上，工作人员离开座位时，应将桌面上含有敏感信息的文件放在抽屉或文件柜内；工作人员离开座位时，终端计算机应退出登录状态、采用屏幕保护口令保护或关机；

c) 关键部位办公环境的要求：在 b）的基础上，在关键区域或部位，应使相应的办公环境与机房的物理位置在一起，以便进行统一的物理保护。

7.2 系统资源管理

7.2.1 资产清单管理

不同安全等级的资产清单管理，有选择地满足以下要求的一项：

a) 一般资产清单：应编制并维护与信息系统相关的资产清单，包括但不限于以下内容：
   1) 信息资产：应用数据、系统数据、安全数据等数据库和数据文档、系统文件、用户手册、培训资料、操作和支持程序、持续性计划、备用系统安排、存档信息；
   2) 软件资产：应用软件、系统软件、开发工具和实用程序；
   3) 有形资产：计算机设备（处理器、监视器、膝上型电脑、调制解调器），通信设备（路由器、数字程控交换机、传真机、应答机），磁媒体（磁带和软盘），其他技术装备（电源、空调设备），家具和机房；
   4) 应用业务相关资产：由信息系统控制的或与信息系统密切相关的应用业务的各类资产，由于信息系统或信息的泄露或破坏，这些资产会受到相应的损坏；
   5) 服务：计算和通信服务，通用设备如供暖、照明、供电和空调等；

b) 详细的资产清单：在 a）的基础上，应清晰识别每项资产的拥有权、责任人、安全分类以及资产所在的位置等；

c) 业务应用系统清单：在 b）的基础上，应清晰识别业务应用系统资产的拥有权、责任人、安全分类以及资产所在的位置等；必要时应该包括主要业务应用系统处理流程和数据流的描述，以及业务应用系统用户分类说明。

7.2.2 资产的分类与标识要求

不同安全等级的资产的分类与标识，有选择地满足以下要求的一项：

a) 资产标识：应根据资产的价值/重要性对资产进行标识，以便可以基于资产的价值选择保护措施和进行资产管理等相关工作；

b) 资产分类管理：在 a）的基础上，应对信息资产进行分类管理，对信息系统内分属不同业务范围的各类信息，按其对安全性的不同要求分类加以标识。对于信息资产，通常信息系统数据可以分为系统数据和用户数据两类，其重要性一般与其所在的系统或子系统的安全保护等级相关；用户数据的重要性还应考虑自身保密性分类，如：
   1) 国家秘密信息：秘密、机密、绝密信息；
   2) 其他秘密信息：受国家法律保护的商业秘密和个人隐私信息；
   3) 专有信息：国家或组织机构内部共享、内部受限、内部专控信息，以及公民个人专有信息；

4) 公开信息：国家公开共享的信息、组织机构公开共享的信息、公民个人可公开共享的信息；组织机构应根据业务应用的具体情况进行分类分级和标识，纳入规范化管理；不同安全等级的信息应当本着“知所必需、用所必需、共享必需、公开必需、互联通信必需”的策略进行访问控制和信息交换管理；

c) 资产体系架构：在 b）的基础上，以业务应用为主线，用体系架构的方法描述信息资产；资产体系架构不是简单的资产清单，而是通过对各个资产之间有机的联系和关系的结构性描述。

7.2.3 介质管理

不同安全等级的介质管理，有选择地满足以下要求的一项：

a) 介质管理基本要求：对脱机存放的各类介质（包括信息资产和软件资产的介质）进行控制和保护，以防止被盗、被毁、被修改以及信息的非法泄漏；介质的归档和查询应有记录，对存档介质的目录清单应定期盘点；介质应储放在安全的环境中防止损坏；对于需要送出维修或销毁的介质，应防止信息的非法泄漏；对各类介质的保管应指定专人保管；

b) 介质异地存放要求：在 a）的基础上，根据所承载的数据和软件的重要程度对介质进行标识和分类，存放在由专人管理的介质库中，防止被盗、被毁以及信息的非法泄漏；对存储保密性要求较高的信息的介质，其借阅、拷贝、传输须经相应级别的领导批准后方可执行，并登记在册；存储介质的销毁必须经批准并按指定方式进行，不应自行销毁；介质应保留 2 个以上的副本，而且要求介质异地存储，存储地的环境要求和管理方法应与本地相同；

c) 完整性检查的要求：在 b）的基础上，对重要介质的数据和软件必要时可以加密存储；对重要的信息介质的借阅、拷贝、分发传递须经相应级别的领导的书面审批后方可执行，各种处理过程应登记在册，介质的分发传递采取保护措施；对于需要送出维修或销毁的介质，应首先删除信息，再重复写操作进行覆盖，防止数据恢复和信息泄漏；需要带出工作环境的介质，其信息应受到保护；对存放在介质库中的介质应定期进行完整性和可用性的检查，确认其数据或软件没有受到损坏或丢失；

d) 加密存储的要求：在 c）的基础上，对介质中的重要数据必须使用加密技术或数据隐藏技术进行存储；介质的保存和分发传递应有严格的规定并进行登记；介质受损但无法执行删除操作的，必须销毁；介质销毁在经主管领导审批后应由两人完成，一人执行销毁一人负责监销，销毁过程应记录；

e) 高强度加密存储的要求：在 d）的基础上，对极为重要数据的介质应该使用高强度的加密技术或数据隐藏技术进行存储，并对有关密钥和数据隐藏处理程序严格保管。

7.2.4 挂载设备管理要求

7.2.4.1 多功能智能杆应能为挂载设备提供杆上必要条件，包括各类挂载设备的安装固定、线缆接入和布设、网络接入、接地与防雷保护等功能。

7.2.4.2 多功能智能杆应能为挂载设备提供所需交流或直流供电接口，宜具备漏电监测、供电监测、远程控制、倾斜监测、积水监测、舱门开关监测等功能。

7.2.4.3 多功能智能杆的设置应统筹用地、建筑、景观、道路空间等规划设计的管控要求，满足所在场景空间的服务功能需求。

7.2.4.4 多功能智能杆外观设计应与当地城市规划设计和所处场景相融合，符合城市规划中对城市风貌的要求。

7.2.4.5 多功能智能杆杆体结构和功能设置应综合考虑搭载设备的工作环境、安装空间、结构承载能力、服务功能稳定性、耐久性（结构、设备、涂装）等因素，技术参数指标应满足杆体所搭载设备正常工作需求。

7.2.4.6 应在经过充分测试评估后，在不影响关键挂载设备、边缘控制器安全稳定运行的情况下进行补丁、固件更新等工作。

7.2.4.7 关键挂载设备、边缘控制器应通过安全传输通道进行固件与补丁更新，在检测到异常时应能将结果上报至安全管理中心。

7.2.4.8 应对挂载设备状态进行监测，当发现不明设备入侵时应及时定位处理。

7.2.4.9 应保证只有授权的多功能智能杆挂载设备可以接入。

7.2.4.10 应能够限制与多功能智能杆挂载设备通信的目的地址，以免来自陌生地址的攻击行为；

7.2.4.11 应能够限制于多功能智能杆场景中与网关节点通信的目的地址，以避免对陌生地址的攻击行为。

7.2.4.12 连接多功能智能杆的边缘控制器应具备对合法连接设备（多功能智能杆挂载设备、路由节点、数据处理中心）进行标识和鉴别的能力，至少支持基于网络标识、MAC 地址、通信协议、通信端口的身份鉴别机制。

7.2.4.13 连接多功能智能杆的边缘控制器应具备过滤非法节点和伪造接地所发送的数据的能力；当检测到流量异常时，应能限制该端口的流量或关闭该端口，并上报异常信息。在异常消除后，应能自动恢复该端口的正常功能。

7.2.4.14 连接多功能智能杆的边缘控制器应具备对合法连接设备（多功能智能杆挂载设备、路由节点、数据处理中心）进行脆弱性（系统漏洞、弱口令）扫描。

7.2.4.15 连接多功能智能杆的边缘控制器检测到攻击行为时，应上报攻击源 IP、攻击类型、攻击时间等信息。

7.3 用户操作管理

7.3.1 用户管理要求

7.3.1.1 用户分类管理

不同安全等级的用户分类管理，有选择地满足以下要求的一项：

a) 用户分类清单：应按审查和批准的用户分类清单建立用户和分配权限。用户分类清单应包括信息系统的所有用户的清单，以及各类用户的权限；用户权限发生变化时应及时更改用户清单内容；

b) 必要时可以对有关用户开启审计功能，用户分类清单应包括：

1) 系统用户：指系统管理员、网络管理员、数据库管理员和系统运行操作员等特权用户；

2) 普通用户：指 OA 和各种业务应用系统的用户；

3) 外部客户用户：指组织机构的信息系统对外服务的客户用户；

4) 临时用户：指系统维护测试和第三方人员使用的用户；

c) 特权用户管理：在 a）的基础上，应对信息系统的所有特权用户列出清单，说明各个特权用户的权限，以及特权用户的责任人员和授权记录；定期检查特权用户的实际分配权限是否与特权用户清单符合；对特权用户开启审计功能；
d) 重要业务用户管理：在 b）的基础上，应对信息系统的所有重要业务用户的列出清单，说明各个用户的权限，以及用户的责任人员和授权记录；定期检查重要业务用户的实际分配权限是否与用户清单符合；对重要业务用户开启审计功能；
e) 关键部位用户管理：在 c）的基础上，应对关键部位用户采取逐一审批和授权的程序，并记录备案；定期检查这些用户的实际分配权限是否与授权符合，对这些用户开启审计功能。

7.3.1.2 系统用户要求

不同安全等级的系统用户，有选择地满足以下要求的一项：
a) 最小授权要求：系统用户应由信息系统的主管领导指定，授权应以满足其工作需要的最小权限为原则；系统用户应接受审计；
b) 责任到人要求：在 a）的基础上，对重要信息系统的系统用户，应进行人员的严格审查，符合要求的人员才能给予授权；对系统用户应能区分责任到个人，不应以部门或组作为责任人；
c) 监督性保护要求：在 b）的基础上，在关键信息系统中，对系统用户的授权操作，必须有两人在场，并经双重认可后方可操作；操作过程应自动产生不可更改的审计日志。

7.3.1.3 普通用户要求

不同安全等级的普通用户，有选择地满足以下要求的一项：
a) 普通用户的基本要求：应保护好口令等身份鉴别信息；发现系统的漏洞、滥用或违背安全行为应及时报告；不应透露与组织机构有关的非公开信息；不应故意进行违规的操作；
b) 处理敏感信息的要求：在 a）的基础上，不应在不符合敏感信息保护要求的系统中保存和处理高敏感度的信息；不应使用各种非正版软件和不可信的自由软件；
c) 重要业务应用的要求：在 b）的基础上，应在系统规定的权限内进行操作，必要时某些重要操作应得到批准；用户应保管好自己的身份鉴别信息载体，不应转借他人。

7.3.1.4 机构外部用户要求

不同安全等级的机构外部用户，有选择地满足以下要求的一项：
a) 外部用户一般要求：应对外部用户明确说明使用者的责任、义务和风险，并要求提供合法使用的声明；外部用户应保护口令等身份鉴别信息；外部用户只能是应用层的用户；
b) 外部特定用户要求：在 a）的基础上，可对特定外部用户提供专用通信通道，端口，特定的应用或数据协议，以及专用设备等；
c) 外部用户的限制：在 b）的基础上，在关键部位，一般不允许设置外部用户。

7.3.1.5 临时用户要求

不同安全等级的临时用户，有选择地满足以下要求的一项：

a) 临时用户的设置与删除：临时用户的设置和期限必须经过审批，使用完毕或到期应及时删除，设置与删除均应记录备案；
b) 临时用户的审计：在设置与删除的基础上，对主要部位的临时用户应进行审计，并在删除前进行风险评估；
c) 临时用户的限制：在审计的基础上，在关键部位，一般不允许设置临时用户。

7.3.2 运行操作管理要求

7.3.2.1 服务器操作管理要求

不同安全等级的服务器操作管理，有选择地满足以下要求的一项：

a) 服务器操作管理基本要求：对服务器的操作应由授权的系统管理员实施；应按操作规程实现服务器的启动/停止、加电/断电等操作；维护服务器的运行环境及配置和服务设定；按 7.3.1.1 的相关要求实现操作的身份鉴别管理；
b) 日志文件和监控管理：在 a）的基础上，加强日志文件管理和监控管理。日志管理包括对操作系统、数据库系统以及业务系统等日志的管理和维护；监控管理包括监控系统性能，如监测 CPU 和内存的利用率、检测进程运行及磁盘使用情况等；
c) 配置文件管理：在 b）的基础上，加强配置文件管理，包括服务器的系统配置和服务设定的配置文件的管理，定期对系统安全性进行有效性评估和检查，及时发现系统的新增缺陷或漏洞。

7.3.2.2 终端计算机操作管理要求

不同安全等级的终端计算机操作管理，有选择地满足以下要求的一项：

a) 终端计算机操作管理基本要求：用户在使用自己的终端计算机时，应设置开机、屏幕保护、目录共享口令；非组织机构配备的终端计算机未获批准，不能在办公场所使用；及时安装经过许可的软件和补丁程序，不应自行安装及使用其它软件和自由下载软件；未获批准，严禁使用 Modem 拨号、无线网卡等方式或另辟通路接入其它网络；身份鉴别机制应按照 7.3.1.1 相关要求处理；
b) 重要部位的终端计算机管理：在 a）的基础上，应有措施防止终端计算机机箱私自开启，如需拆机箱应在获得批准后由相关管理部门执行；接入保密性较高的业务系统的终端计算机不应直接接入低级别系统或网络；
c) 关键部位的终端计算机管理：在 b）的基础上，终端计算机必须启用两个及两个以上身份鉴别技术的组合来进行身份鉴别；终端计算机应采用低辐射设备；每个终端计算机的管理必须由专人负责，如果多人共用一个终端计算机，应保证各人只能以自己的身份登录，并采用的身份鉴别机制。

7.3.2.3 网络及安全设备操作管理要求

不同安全等级的网络及安全设备操作的管理，有选择地满足以下要求的一项：

a) 网络及安全设备操作基本要求：对网络及安全设备的操作应由授权的系统管理员实施；应按操作规程实现网络设备和安全设备的接入/断开、启动/停止、加电/断电等操作；维护网络和安全设备的运行环境及配置和服务设定；对实施网络及安全设备操作的管理员应按 7.3.1.1 的要求进行身份鉴别；

b) 策略配置及检查：在 a）的基础上，管理员应按照安全策略要求进行网络及设备配置；应定期检查实际配置与安全策略要求的符合性；
c) 安全机制集中管理控制：在 b）的基础上，应通过安全管理控制平台等设施对网络及安全设备的安全机制进行统一控制、统一管理、统一策略，保障网络正常运行。

7.3.2.4 业务应用操作管理要求

不同安全等级的业务应用操作管理，有选择地满足以下要求的一项：

a) 业务应用操作程序和权限控制：业务应用系统应按 7.3.1.1 的要求对操作人员进行身份鉴别；挂载设备的安全管理应符合 7.2.4 的要求；业务应用系统应能够以菜单等方式限制操作人员的访问权限；业务应用操作程序应形成正式文档，需要进行改动时应得到管理层授权；这些操作步骤应指明具体执行每个作业的指令，包括但不限于以下内容：
   1) 指定需要处理和使用的信息；
   2) 明确操作步骤，包括与其它系统的相互依赖性、操作起始和结束的时间；
   3) 说明处理错误或其它异常情况的指令，系统出现故障时进行重新启动和恢复的措施，以及在出现意外的操作或技术问题时需要技术支持的联系方法。
b) 业务应用操作的限制：在 a）的基础上，对重要的业务应用操作应根据特别许可的权限执行；业务应用操作应进行审计；
c) 业务应用操作的监督：在 b）的基础上，关键的业务应用操作应有 2 人同时在场或同时操作，并对操作过程进行记录。

7.3.2.5 变更控制和重用管理要求

不同安全等级的变更控制和重用管理，有选择地满足以下要求的一项：

a) 变更控制的申报和审批：任何变更控制和设备重用必须经过申报和审批才能进行，同时还应注意以下要求：
   1) 注意识别重大变更，并进行记录；
   2) 评估这些变更的潜在影响；
   3) 向所有相关人员通报变更细节；
   4) 明确中止变更并从失败变更中恢复的责任和处理方法；
   5) 重用设备中原有信息的清除。
b) 制度化的变更控制：在 a）的基础上，制度化的变更控制和设备重用还应包括：对操作系统、数据库、应用系统、人员、服务等的变更控制应制度化；对所有计划和制度执行情况进行定期或不定期的检查；对安全策略和管理计划的修订；对基于变更和设备重用的各种规章制度的修订和完善；建立运行过程管理文档，书面记录相关的管理责任及工作程序；
c) 变更控制的一致性管理：在 b）的基础上，一致性的变更控制和设备重用还应包括：对信息系统的任何变更必须考虑全面安全事务一致性；更改方案应得到系统主管领导的审批；操作系统与应用系统的控制更改程序应相互配合；通过审计日志和过程记录，记载更改中的所有有关信息；更改后将变更结果书面通知所有有关部门和人员，以便进行相应的调整；

d) 变更控制的安全审计：在 c）的基础上，变更控制的安全审计还应包括：建立系统更改操作的审批程序和操作流程，防止随意更改而开放危险端口或服务；对重要的变更控制应实施独立的安全审计，并对全面安全事务一致性进行检查和评估；系统更改的日志记录和设备重用记录应妥善保存；
e) 变更的安全评估：在 d）的基础上，变更控制的安全审计还应包括：针对所有变更和设备重用进行安全评估；应采取相应保证措施，对变更计划和效果进行持续改善。

7.3.2.6 信息交换管理要求

不同安全等级的信息交换管理，有选择地满足以下要求的一项：
a) 信息交换的基本管理：在信息系统上公布信息应符合国家有关政策法规的规定；对所公布的信息应采取适当的安全措施保护其完整性；应保护业务应用中的信息交换的安全性，防止欺诈、合同纠纷以及泄露或修改信息事件的发生；
b) 信息交换的规范化管理：在 a）的基础上，还应包括在组织机构之间进行信息交换应建立安全条件的协议，根据业务信息的敏感度，明确管理责任，以及设备、平台、用户之间数据传输的最低安全要求；
c) 不同安全区域之间信息传输的管理：在 b）的基础上，还应包括对于信息系统内部不同安全区域之间的信息传输，应有明确的安全要求；
d) 高安全信息向低安全区域传输的管理：在 c）的基础上，还应包括对高安全信息向低安全区域的传输应经过组织机构领导层的批准，明确部门和人员的责任，并采取的安全专控措施。

数据格式、数据传输、数据共享、数据应用的安全

7.4 运行维护管理

7.4.1 日常运行安全管理

不同安全等级的日常运行安全管理，有选择地满足以下要求的一项：
a) 系统运行的基本安全管理：应通过正式授权程序委派专人负责系统运行的安全管理；应建立运行值班等有关安全规章制度；应为信息系统可靠运行而实施各种检测、监控、审计、分析、备份和容错；应对运行安全进行监督检查；应明确各个岗位人员对信息系统各类资源的安全责任；应明确信息系统安全管理人员和普通用户对信息系统资源的访问权限；对信息系统中数据管理应保证技术上能够达到 GB/T 20271—2006 中 6.1.3 的有关要求；
b) 系统运行的制度化管理：在 a）的基础上，应按风险管理计划和操作规程定期对信息系统的运行进行风险分析与评估，并向管理层提交正式的风险分析报告。为此应实行系统运行的制度化管理，包括：
   1) 对系统的数据格式安全、数据传输安全、数据共享安全、数据应用安全和病毒防护的使用制定管理规定；
   2) 制定应用软件安全管理规章制度，应用软件的采购应经过批准，对应用软件的安全性应进行调查，不运行未经验证的软件；对应用软件的使用采取授权管理，没有得到许可的用户不应安装、调试、运行、卸载应用软件，并对应用软件的使用进行审计；

3) 制定外部服务方对信息系统访问的安全制度，对外部服务方访问系统可能发生的安全性进行评估，采取安全措施对访问实施控制，与外部服务方签署安全保密合同，并要求有关合同不违背总的安全策略；
4) 安全管理负责人应会同信息系统应用各方制定应急计划和灾难恢复计划，以及实施规程，并进行必要验证、按照等级保护要求定期开展演练和技术培训；
5) 对所需外部资源的应急计划要与有关各方签署正式合同，合同中应规定服务质量，并包括安全责任和保密条款；
6) 制定安全事件处理规程，保证在短时间内能够对安全事件进行处理；
7) 制定信息系统的数据备份制度，要求指定专人负责备份管理，保证信息系统自动备份和人工备份的准确性、可用性；
8) 制定有关变更控制制度，保证变更后的信息系统能满足既定的安全目标；
9) 制定运行安全管理检查制度，定期或不定期对所有计划和制度执行情况进行监督检查，并对安全策略和管理计划进行修订；接受上级或国家有关部门对信息系统安全工作的监督和检查；
10) 根据组织机构和信息系统出现的各种变化及时修订、完善各种规章制度；
11) 建立严格的运行过程管理文档，其中包括责任书、授权书、许可证、各类策略文档、事故报告处理文档、安全配置文档、系统各类日志等，并保证文档的一致性；
12) 对信息系统中数据管理应保证技术上能够达到 GB/T 20271—2006 中 6.2.3 的有关要求；

c) 系统运行的风险控制：在 b）的基础上，使用规范的方法对信息系统运行的有关方面进行风险控制，包括要求对关键岗位的人员实施严格的背景调查和管理控制，切实落实最小授权原则和分权制衡原则，关键安全事务要求双人共管；对外部服务方实施严格的访问控制，对其访问实施监视，并定期对外部服务方访问的风险进行分析和评估；要求有专人负责应急计划和灾难恢复计划的管理工作，保证应急计划和灾难恢复计划有效执行；要求系统中的关键设备和数据采取可靠的备份措施；要求保证各方面安全事务管理的一致性；对信息系统中数据管理应保证技术上能够达到 GB/T 20271—2006 中 6.3.3 的有关要求；
d) 系统运行的安全审计：在 c）的基础上，应建立风险管理质量管理体系文件，并对系统运行管理过程实施独立的审计，保证安全管理过程的有效性；信息系统生存周期各个阶段的安全管理工作应有明确的目标、明确的职责，实施独立的审计；应对病毒防护管理制度实施定期和不定期的检查；应对外部服务方每次访问信息系统的风险进行控制，实施独立的审计；定期对应急计划和灾难恢复计划的管理工作进行评估；对使用单位的安全策略、安全计划等安全事务的一致性进行检查和评估；对信息系统中数据管理应保证技术上能够达到 GB/T 20271—2006 中 6.4.3 的有关要求；
e) 系统运行的全面安全管理：在 d）的基础上，应将风险管理作为机构业务管理的组成部分，对风险管理活动和信息系统生存周期各个阶段的安全实施全面管理；应制定全面的应急计划和灾难恢复计划管理细则，并通过持续评估，保证应急计划和灾难恢复计划的有效性；应对所有变更进行安全评估，保证变更控制计划的不断完善；对信息系统中数据管理应保证技术上能够达到 GB/T 20271—2006 中 6.5.3 的有关要求。

7.4.2 运行状况监控要求

不同安全等级的运行状况监控，有选择地满足以下要求的一项：

a) 日志管理：所有的系统日志应保留一定期限，不能被改变，只允许授权用户访问；日志应有脱机保存的介质；信息系统应使用统一的时间，以确保记录日志准确；日志应定期处理并产生报告；审计日志须经授权方可查阅；应告知用户某些行为是会被审计的；
b) 监视服务器安全性能：在 a）的基础上，监视与安全机制相关的服务器性能变化，包括：监测 CPU 和内存的利用率；检测进程运行，发现对资源消耗大的进程，并提出解决方案；监测磁盘使用情况，主要是指数据库的容量变化和日志文件的大小变化；
c) 监视网络安全性能：在 b）的基础上，应建立信息系统安全机制集中管理机构完成网络安全性能和其他信息的监视；
d) 对关键区域的监视：在 c）的基础上，安全机制集中管理机构应对关键区域和关键业务应用系统运行的监视，并与主管部门共同制定具体的管理办法；
e) 对核心数据的监视：在 d）的基础上，安全机制集中管理机构应对关键区域和关键业务应用系统核心数据进行监视，并与主管部门共同制定具体的管理办法，经上一级负责人的批准执行。

7.4.3 软件硬件维护管理要求

不同安全等级的软件和硬件维护管理，有选择地满足以下要求的一项：

a) 软件、硬件维护的责任：应明确信息系统的软件、硬件维护的人员和责任，规定维护的时限，以及设备更新和替换的管理办法；制定有关软件、硬件维修的制度；
b) 涉外维修的要求：在 a）基础上，对需要外出维修的设备，应经过审批，磁盘数据应进行删除；外部维修人员进入机房维修，应经过审批，并有专人负责陪同；
c) 可监督的维修过程：在 b）基础上，应对重要区域的数据和软件系统进行必要的保护，防止因维修造成破坏和泄漏；应对维修过程及有关现象记录备案；
d) 强制性的维修管理：在 c）基础上，一般不应允许外部维修人员进入关键区域；应根据维修方案和风险评估的结果确定维修方式，可采用更新设备的方法解决。

7.4.4 外部服务方访问管理要求

不同安全等级的对外部服务方访问管理，有选择地满足以下要求的一项：

a) 外部服务方访问的审批控制：对外部服务方访问的要求，应经过相应的申报和审批程序；
b) 外部服务方访问的制度化管理：在 a）的基础上，应对外部服务方访问建立相应的安全管理制度；外部服务方访问应签署保密合同；
c) 外部服务方访问的风险评估：在 b）的基础上，应对外部服务方访问进行风险分析和评估；应对外部服务方访问实施严格控制；应对外部服务方访问实施监视；
d) 外部服务方访问的强制管理：在 c）的基础上，在重要安全区域，应对外部服务方每次访问进行风险控制；必要时应外部服务方的访问进行限制。

7.5 外包服务管理

7.5.1 外包服务合同

外包服务合同基本要求：对由组织机构外部服务商承担完成的外包服务，应签署正式的书面合同，包括但不限于以下内容：

a） 对符合法律要求的说明，如数据保护法规；
b） 对外包服务的风险的说明，包括风险的来源、具体风险描述和风险的影响，明确如何维护并检测组织的业务资产的完整性和保密性；
c） 对外包服务合同各方的安全责任界定，应确保外包合同中的参与方（包括转包商）都了解各自的安全责任；
d） 对控制安全风险应采用的控制措施的说明，包括物理和逻辑两个方面，应明确使用何种物理和逻辑控制措施，限制授权用户对系统内业务敏感信息的访问，以及为外包出去的设备提供何种级别的物理安全保护；
e） 对外包服务风险发生时应采取措施的说明，如在发生灾难事故时，应如何维护服务的可用性；
f） 对外包服务的期限、中止的条件和善后处理的事宜以及由此产生责任问题的说明；
g） 对审计人员权限的说明。

7.5.2 外包服务商

不同安全等级的对外包服务商，有选择地满足以下要求的一项：

a） 外包服务商的基本要求：应选择具有相应服务资质并信誉好的外包服务商；
b） 在既定的范围内选择外包服务商：对较为重要的业务应用，应在行业认可或者是经过上级主管部门批准的范围内，选择具有相应服务资质并信誉好的可信的外包服务商；
c） 外包服务的限制要求：关键的或涉密的业务应用，一般不应采用外包服务方式。

7.5.3 外包服务的运行管理

不同安全等级的外包服务的运行管理，有选择地满足以下要求的一项：

a） 外包服务的监控：对外包服务的业务应用系统运行的安全状况应进行监控和检查，出现问题应遵照合同规定及时处理和报告；
b） 外包服务的评估：在 a）的基础上，对外包服务的业务应用系统运行的安全状况应定期进行评估，当出现重大安全问题或隐患时应进行重新评估，提出改进意见，直至停止外包服务。

7.6 安全机制管理

7.6.1 身份鉴别机制管理要求

不同安全等级的身份鉴别机制的管理，有选择地满足以下要求的一项：

a） 身份鉴别机制管理基本要求：对网络、操作系统、数据库系统等系统管理员和应用系统管理员以及普通用户，应明确使用和保护身份鉴别机制的责任；应指定安全管理人员定期进行检查，对身份鉴别机制的管理应保证 GB/T 20271—2006 中 6.1.3.1 所采用的安全技术能达到其应有的安全性要求；
b） 身份鉴别机制增强要求：在 a）的基础上，应采用不可伪造的鉴别信息进行身份鉴别；鉴别信息应进行相应的保护；对身份鉴别机制的管理应保证 GB/T 20271—2006 中 6.2.3.1 所采用的安全技术能达到其应有的安全性要求；

c） 身份鉴别和认证系统的管理维护：在 b）的基础上，应采用有关身份鉴别和认证系统的管理维护措施；对身份鉴别机制的管理应保证 GB/T 20271—2006 中 6.3.3.1 所采用的安全技术能达到其应有的安全性要求；

d） 身份鉴别和认证管理的强制保护：在 c）的基础上，应采用多鉴别机制进行身份鉴别，操作过程需要留有操作记录和审批记录，必要时应两人以上在场才能进行；对身份鉴别机制的管理应保证 GB/T 20271—2006 中 6.4.3.1 所采用的安全技术能达到其应有的安全性要求；

e） 身份鉴别和认证管理的专项管理：在 d）的基础上，与相关业务部门共同制定专项管理措施；对身份鉴别机制的管理应保证 GB/T 20271—2006 中 6.5.3.1 所采用的安全技术能达到其应有的安全性要求。

7.6.2 访问控制机制管理要求

不同安全等级的访问控制机制管理，有选择地满足以下要求的一项：

a） 自主访问控制机制的管理：应根据自主访问控制机制的要求，由授权用户为主、客体设置相应访问的参数；

b） 自主访问控制审计管理：在 a）基础上，应将自主访问控制与审计密切结合，实现对自主访问控制过程的审计，使访问者必须为自己的行为负责；并保证最高管理层对自主访问控制管理的掌握；

c） 强制访问控制的管理：在 b）基础上，应将强制访问控制与审计密切结合，实现对强制访问控制过程的审计；应根据强制访问控制机制的要求，由授权的安全管理人员通过专用方式为主、客体设置标记信息；可采用集中式、分布式和混合式等基本的访问控制管理模式，对分布在信息系统的不同计算机系统上实施同一安全策略的访问控制机制，设置一致的主、客体标记信息；应根据信息系统的安全需求，确定实施系统级、应用级、用户级的审计跟踪；

d） 访问控制的监控管理：在 c）基础上，对访问控制进行监控管理，对系统、用户或环境进行持续性检查；对实时性强的活动加强监控，包括每日或每周对审计跟踪（如有关非法登录尝试）的检查；注意保护和检查审计跟踪数据，以及用于审计跟踪分析的工具；

e） 访问控制的专项控制：在 d）基础上，应具有严格的用户授权与访问控制措施；对访问控制机制的设置进行专项审批，并由独立的安全管理人员对网络、系统和应用等方面的访问控制机制进行独立的有效性评估和检查。

7.6.3 管理平台安全管理要求

不同安全等级的多功能智能杆管理平台操作系统和公共数据的安全管理，有选择地满足以下要求的一项：

a） 管理平台操作系统安全管理基本要求：应对不同安全级别的操作系统和数据库管理系统按其安全技术和机制的不同要求实施相应的安全管理；应通过正式授权程序委派专人负责系统安全管理；建立系统安全配置、备份等安全管理规章制度；按规章制度的要求进行正确的系统安全配置、备份等操作，及时进行补丁升级；

b） 基于审计的管理平台操作系统安全管理要求：在 a）的基础上，应对系统进行日常安全管理，包括对用户安全使用进行指导和审计等；应依据操作规程确定审计事件、审

计内容、审计归档、审计报告；对授权用户应采用相应身份鉴别机制（见 7.6.1）进行鉴别，并遵照规定的登录规程登录系统和使用许可的资源；应对系统工具的使用进行授权管理和审计；应对系统的安全弱点和漏洞进行控制；应依据变更控制规程对系统的变更进行控制；应及时对系统资源和系统文档进行安全备份；

c) 基于标记的管理平台操作系统安全管理要求：在 b）的基础上，应根据访问控制安全策略的要求，全面考虑和统一设置、维护用户及主、客体的标记信息；设置和维护标记信息的操作应由授权的系统安全员通过系统提供的安全员操作界面实施；对可能危及系统安全的系统工具进行严格的控制；应制定严格的变更控制制度，保证变更不影响应用系统的可用性、安全性，保证变更过程的有效性、可审计性和可恢复性；应对操作系统资源和系统文档进行标记、安全备份，并制定、实施应急安全计划；

d) 基于强制的管理平台操作系统安全管理要求：在 c）的基础上，应按系统内置角色强制指定系统安全管理责任人；应保证系统管理过程的可审计性；应定期对操作系统安全性进行评估；

e) 基于专控的管理平台操作系统安全管理要求：在 d）的基础上，应保证系统的安全管理工作在多方在场并签署责任书情况下进行；应使用经过验证的系统软件，确保使用者熟悉系统的操作流程，并对操作人员的操作过程实施监视。

7.6.4 网络安全管理要求

不同安全等级的网络安全管理，有选择地满足以下要求的一项：

a) 网络安全管理基本要求：应对不同安全级别的网络按其安全技术和机制的不同要求实施相应的安全管理；应通过正式授权程序指定网络安全管理人员；应制定有关网络系统安全管理和配置的规定，保证安全管理人员按相应规定对网络进行安全管理；

b) 基于规程的网络安全管理：在 a）的基础上，应按有关规程对网络安全进行定期评估，不断完善网络安全策略，建立、健全网络安全管理规章制度，包括：

   1) 制定使用网络和网络服务的策略。依据总体安全方针、策略制定允许提供的网络服务、制定网络访问许可和授权管理制度、保证信息系统网络连接和服务的安全技术正确实施；

   2) 制定网络安全教育和培训计划，保证信息系统的各类用户熟知自己在网络安全方面的安全责任和安全规程；

   3) 建立网络访问授权制度，保证经过授权的用户才能在指定终端，使用指定的安全措施，按设定的可审计路由访问许可的网络服务；

   4) 对安全区域外部移动用户的网络访问实施严格的审批制度，实施用户安全认证和审计技术措施，保证网络连接的可靠性、保密性，保证用户对外部连接的安全性负责；

   5) 定义与外部网络连接的接口边界，建立安全规范，定期对外部网络连接接口的安全进行评估，对通过外部连接的可信信息系统之间的网络信息提供加密服务，有关加密设备和算法的使用按国家有关规定执行；

   6) 对外进行公共服务的信息系统，应采取严格的安全措施实施访问控制，保证外部用户对服务的访问得到控制和审计，并保证外部用户对特定服务的访问不危及内部信息系统的安全，对外传输的数据和信息要经过审查，防止内部人员通过内外网的边界泄露敏感信息；

7) 多功能智能杆各个子功能的使用边界安全，需要明确定义各个子功能的范围和限制，制定数据隔离和访问控制措施，采用安全的协议和加密技术；
8) 对可能从内部网络向外发起的连接资源（如 Modem 拨号接入 Internet）实施严格控制，建立连接资源使用授权制度，建立检查制度防止信息系统使用未经许可和授权的连接资源；
9) 不同安全保护等级的信息系统网络之间的连接，应按访问控制策略实施可审计的安全措施，如使用防火墙、安全路由器等，实现必要的网络隔离；
10) 保证网络安全措施的日常管理责任到人，并对网络安全措施的使用进行审计；
11) 按网络设施和网络服务变更控制制度执行网络配置变更控制；
12) 建立网络安全事件、事故报告处理流程，保证事件和事故处理过程的可审计性；
13) 对网络连接、网络安全措施、网络设备及操作规程定期进行安全检查和评估，提交正式的网络安全报告；
14) 信息系统的关键网络设备设施应有必要的备份。

c) 基于标记的网络安全管理：在 b）的基础上，针对网络安全措施的使用建立严格的审计、标记制度，保证安全措施配有具体责任人负责网络安全措施的日常管理；指定网络安全审计人员，负责安全事件的标记管理，网络安全事件的审计；对审计活动进行控制，保证网络设施或审计工具提供的审计记录完整性和可用性；对可用性要求高的网络指定专人进行不间断的监控，并能及时处理安全事故；
d) 基于强制监督的网络安全管理：在 c）的基础上，建立的独立安全审计，对网络服务、网络安全策略、安全控制措施进行有效性检查和监督；保证网络安全管理人员达到相应的资质；信息系统网络之间的连接应使用可信路径；
e) 基于专控的网络安全管理：在 d）的基础上，要求至少有两名网络安全管理人员实施网络安全管理事务，并保证网络安全管理本身的安全风险得到控制；信息系统网络之间的连接严格控制在可信的物理环境范围内。

7.6.5 挂载设备安全管理要求

不同安全等级的挂载设备安全管理，有选择地满足以下要求的一项：

a) 应用系统安全管理基本要求：应对不同安全级别的应用系统按其安全技术和机制的不同要求实施相应的安全管理；应通过正式授权程序委派专人负责应用系统的安全管理，应明确管理范围、管理事务、管理规程，以及应用系统软件的安全配置、备份等安全工作；应结合业务需求制定相关规章制度，并严格按照规章制度的要求实施应用系统安全管理；
b) 基于操作规程的应用系统安全管理：在 a）的基础上，应制定并落实应用系统的安全操作规程，包括：
1) 指定信息安全管理人员，依据信息安全操作规程，负责信息的分类管理和发布；
2) 对任何可能超越系统或应用程序控制的实用程序和系统软件都应得到正式的授权和许可，并对使用情况进行登记。保证对应用系统信息或软件的访问不影响其他信息系统共享信息的安全性；
3) 应用系统的内部用户，包括支持人员，应按照规定的程序办理授权许可，并根据信息的敏感程度签署安全协议，保证应用系统数据的保密性、完整性和可用性；
4) 应指定专人负责应用系统的审计工作，保证审计日志的准确性、完整性和可用性；

5） 组织有关人员定期或不定期对应用系统的安全性进行审查，并根据应用系统的变更或风险变化提交正式的报告，提出安全建议；
6） 对应用系统关键岗位的工作人员实施资质管理，保证人员的可靠性和可用性；
7） 制定切实可用的应用系统及数据的备份计划和应急计划，并由专人负责落实和管理；
8） 制定应用软件安全管理规章制度，包括应用软件的开发和使用等管理；

c） 基于标记的应用系统安全管理：在 b）的基础上，应对应用软件的使用采取授权、标记管理制度；未授权用户不应安装、调试、运行、卸载应用软件，并对应用软件的使用进行审计；应定期或不定期对应用系统的安全性进行评估，并根据应用系统的变更或风险变化提交正式的评估报告，提出安全建议，修订、完善有关安全管理制度和规程；应用系统的开发人员不应参与应用系统日常运行和安全审计工作；操作系统的管理人员不应参与应用系统的安全配置管理和应用管理；

d） 基于强制的应用系统安全管理：在 c）的基础上，要求建立独立的应用安全审计，对应用系统的总体安全策略、应用系统安全措施的设计、部署、维护和运行管理进行检查；审计人员仅实施审计工作，不参与系统的其它任务，确保授权用户范围内的使用，防止信息的泄漏；

e） 基于专控的应用系统安全管理：在 d）的基础上，应对应用系统的安全状态实施周期更短的审计、检查和操作过程监督，并保证对应用系统的安全措施能适应安全环境的变化；应与应用系统主管部门共同制定专项安全措施。

7.6.6 病毒防护管理要求

不同安全等级的病毒防护管理，有选择地满足以下要求的一项：

a） 病毒防护管理基本要求：通过正式授权程序对病毒防护委派专人负责检查网络和主机的病毒检测并保存记录；使用外部移动存储设备之前应进行病毒检查；要求从不信任网络上所接收的文件或邮件，在使用前应首先检查是否有病毒；及时升级防病毒软件；定期进行总结汇报病毒安全状况；

b） 基于制度化的病毒防护管理：在 a）的基础上，制定并执行病毒防护系统使用管理、应用软件使用授权安全管理等有关制度；应检查网络内计算机病毒库的升级情况并进行记录；对非在线的内部计算机设备及其它移动存储设备，以及外来或新增计算机做到入网前进行杀毒和补丁检测；

c） 基于集中实施的病毒防护管理：在 b）的基础上，实行整体网络统一策略、定期统一升级、统一控制，紧急情况下增加升级次数；对检测或截获的各种高风险病毒进行及时分析处理，提供相应的报表和总结汇报；采取对系统所有终端有效防范病毒或恶意代码引入的措施；

d） 基于监督检查的病毒防护管理：在 c）的基础上，针对病毒防护管理制度执行情况，以及病毒防护的安全情况，进行定期或不定期检查。

7.6.7 密码管理要求

不同安全等级的密码管理，有选择地满足以下要求的一项：

a） 密码算法和密钥管理：应按国家密码主管部门的规定，对信息系统中使用的密码算法和密钥进行管理；应按国家有关法律法规要求，对信息系统中包含密码的软、硬件信

息处理模块的进、出口进行管理；应按国家密码主管部门的规定，对密码算法和密钥实施分等级管理；

b) 以密码为基础的安全机制的管理：在 a）的基础上，应对信息系统中以密码为基础的安全机制实施分等级管理。

7.7 业务连续性管理

7.7.1 数据备份与恢复管理要求

不同安全等级的数据备份和恢复，有选择地满足以下要求的一项：

a) 数据备份的内容和周期要求：应明确说明需定期备份重要业务信息、系统数据及软件等内容和备份周期；确定重要业务信息的保存期以及其它需要保存的归档拷贝的保存期；采用离线备份或在线备份方案，定期进行数据增量备份；可使用手工或软件产品进行备份和恢复；对数据备份和恢复的管理应保证 GB/T 20271—2006 中 6.1.2.4 所采用的安全技术能达到其应有的安全性要求；

b) 备份介质及其恢复的检查要求：在 a）的基础上，应进行数据和局部系统备份；定期检查备份介质，保证在紧急情况时可以使用；应定期检查及测试恢复程序，确保在预定的时间内正确恢复；应根据数据的重要程度和更新频率设定备份周期；应指定专人负责数据备份和恢复，并同时保存几个版本的备份；对数据备份和恢复的管理应保证 GB/T 20271—2006 中 6.2.2.5 所采用的安全技术能达到其应有的安全性要求；

c) 备份和恢复措施的强化管理：在 b）的基础上，必要时应采用热备份方式保存数据，同时定期进行数据增量备份和应用环境的离线全备份；应分别指定专人负责不同方式的数据备份和恢复，并保存必要的操作记录；对数据备份和恢复的管理应保证 GB/T 20271—2006 中 6.3.2.6 所采用的安全技术能达到其应有的安全性要求；

d) 关键备份和恢复的操作过程监督，在 c）的基础上，根据数据实时性和其他安全要求，采用本地或远地备份方式，制定适当的备份和恢复方式以及操作程序，必要时对备份后的数据采取加密或数据隐藏处理，操作时要求两名工作人员在场并登记备案；对数据备份和恢复的管理应保证 GB/T 20271—2006 中 6.4.2.6 所采用的安全技术能达到其应有的安全性要求。

e) 建立数据销毁策略和管理制度，明确销毁数据范围和流程，记录数据删除的操作时间、操作人、操作方式、数据内容等相关信息。数据在持有期限到期后应当销毁，禁止超期保存数据。

7.7.2 设备和系统的备份与冗余

不同安全等级对设备和系统的备份与冗余应有选择地满足以下要求的一项：

a) 设备备份要求：应实现设备备份与容错；指定专人定期维护和检查备份设备的状况，确保需要接入系统时能够正常运行；应根据实际需求限定备份设备接入的时间；

b) 系统热备份与冗余要求：在 a）的基础上，应实现系统热备份与冗余，并指定专人定期维护和检查热备份和冗余设备的运行状况，定期进行切换试验，确保需要时能正常运行；应根据实际需求限定系统热备份和冗余设备切换的时间；

c) 系统远地备份要求：在 b）的基础上，选择远离市区的地方或其他城市，建立系统远地备份中心，确保主系统在遭到破坏中断运行时，远地系统能替代主系统运行，保证信息系统所支持的业务系统能按照需要继续运行。

7.7.3 安全事件划分管理

不同安全等级对安全事件划分，有选择地满足以下要求的一项：

a) 安全事件内容和划分：安全事件是指信息系统五个层面所发生的危害性情况，包括事故、故障、病毒、黑客攻击性活动、犯罪活动、信息战等；通常可能包括但不限于不可抗拒的事件、设备故障事件、病毒爆发事件、外部网络入侵事件、内部信息安全事件、内部误用和误操作等事件。安全事件的处置需要贯穿整个安全管理的全过程，应依据安全事件对信息系统的破坏程度、所造成的社会影响及涉及的范围，确定具体信息系统安全事件处置等级的划分原则；

b) 安全事件处置制度：在 a）的基础上，建立信息安全事件分等级响应、处置的制度；根据不同安全保护等级的信息系统中发生的各类事件制定相应的处置预案，确定事件响应和处置的范围、程度及适用的管理制度等；信息安全事件发生后，按预案分等级进行响应和处置；在发现或怀疑系统或服务出现安全漏洞或受到威胁时，应按照安全事件处置要求处理；

c) 安全事件管理程序：在 b）的基础上，应明确安全事件管理责任，制定相关程序，应考虑以下要求：

   1) 制定处理预案：针对各种可能发生的安全事件制定相应的处理预案；
   2) 分析原因：注意分析和鉴定事件产生的原因，制定防止再次发生的补救措施；
   3) 收集证据：收集审计记录和类似证据，包括内部问题分析，用作与可能违反合同或违反规章制度的证据；
   4) 处理过程控制：严格控制恢复过程和人员，只有明确确定身份和获得授权的人员才允许访问正在使用的系统和数据，详细记录采取的所有紧急措施，及时报告有关部门，并进行有序的审查，以最小的延误代价确认业务系统和控制的完整性；
   5) 总结吸取教训：对发生的安全事件的类型、规模和损失进行量化和监控；用来分析重复发生的或影响很大的事故或故障，改进控制措施降低事故发生的频率和损失；
   6) 责任划分和追究：应对安全事件的有关管理或执行责任或者责任范围进行划分和追究，使得没有人在其责任范围内所犯的错误能够逃脱检查。

7.7.4 安全事件报告和响应管理

不同安全等级的安全事件报告和响应，有选择地满足以下要求的一项：

a) 安全事件报告和处理程序：信息安全事件实行分等级响应、处置的制度；安全事件应尽快通过适当的管理渠道报告，制定正式的报告程序和事故响应程序；使所有员工知道报告安全事件程序和责任；信息安全事件发生后，根据其危害和发生的部位，迅速确定事件等级，并根据等级启动相应的响应和处置预案；事件处理后应有相应的反馈程序；

b) 安全隐患报告和防范措施：在 a）的基础上，增加对安全弱点和可疑事件进行报告；告知员工未经许可测试弱点属于滥用系统；对于还不能确定为事故或者入侵的可疑事件应报告；对于所有安全事件的报告应记录在案归档留存；

c) 强化安全事件处理的责任：在 b）的基础上，要求安全管理机构或职能部门负责接报安全事件报告，并及时进行处理，注意记录事件处理过程；对于重要区域或业务应用

发生的安全事件，应注意控制事件的影响；应追究安全事件发生的技术原因和管理责任，写出处理报告，并进行必要的评估。

7.7.5 应急处理要求

7.7.5.1 应急处理和灾难恢复管理

不同安全等级的应急处理和灾难恢复，有选择地满足以下要求的一项：

a) 应急处理的基本要求：应对信息系统的应急处理有明确的要求，制定具体的应急处理措施；安全管理人员应协助分管领导落实应急处理措施；
b) 应急处理的制度化要求：在 a）的基础上，应制定总体应急计划和灾难恢复计划并由应急处理小组负责落实；制定针对关键应用系统和支持系统的应急计划和灾难恢复计划并进行测试；对计划涉及人员进行培训，保证这些人员具有相应执行能力；与应急需要外部有关单位应签订合同；制定安全事件处理制度；制定系统信息和文档备份制度等等；
c) 应急处理的检查要求：在 b）的基础上，信息安全领导小组应有人负责或指定专人负责应急计划和实施恢复计划管理工作；信息系统安全机制集中管理机构应协助应急处理小组负责具体落实；检查或验证应急计划和灾难恢复计划，保证应急计划和灾难恢复计划能够有效执行；
d) 应急处理的强制保护要求：在 c）的基础上，针对应急计划和灾难恢复计划实施进行独立审计；针对应急计划和灾难恢复计划进行定期评估，不断改进和完善；
e) 应急处理的持续改进要求：在 d）的基础上，制定包括全面管理细则的应急计划和灾难恢复计划；基于应急计划和灾难恢复计划和安全策略，进行可验证的操作过程监督。

7.7.5.2 应急计划管理

不同安全等级的应急计划，包括但不限于以下内容：

a) 制定应急计划策略，明确制定应急计划所需的职权和相应的管理部门；
b) 进行业务影响分析，识别关键信息系统和部件，确定优先次序；
c) 确定防御性控制，减小系统中断的影响，提高系统的可用性；注意采取措施，减少应急计划生存周期费用；
d) 制定恢复策略，确保系统可以在中断后快速和有效的恢复；
e) 制定信息系统应急计划，包括恢复受损系统所需的指导方针和规程；
f) 计划测试，定期进行培训和演练；
g) 计划维护，有规律地更新适应系统发展；
h) 制定灾难备份计划，以及启动方式。

7.7.5.3 应急计划的实施保障

不同安全等级应急计划的实施保障，有选择地满足以下要求的一项：

a) 应急计划的责任要求：应对明确应急计划的组织和实施人员，使其知道在应急计划实施过程中各自的责任；
b) 应急计划的能力要求：在 a）的基础上，对系统相关的人员进行培训，知道如何以及何时使用应急计划中的控制手段及恢复策略，保证执行应急计划应具有的能力；

c) 应急计划的系统化管理：在 b）的基础上，进行系统化管理用于实施和维护整个组织的应急计划体系，并记录计划实施过程；确保应急计划的执行有足够资源的保证；
d) 应急计划的监督措施：在 c）的基础上，从风险评估开始，考虑所有的运行管理过程，识别可能引起业务过程中断的事件，应有业务资源和业务过程管理者的参与和监督；
e) 应急计划的持续改进：在 d）的基础上，应针对计划的正确性和完整性进行定期检查，在计划发生重大变化时应立即检查；根据业务应用的重要程度的不同，不断对计划内容和规程进行评估和完善。