网络安全运维管理规范

目 录

[第一章 环境安全 1](#_Toc134518001)

[第二章 信息资产管理 4](#_Toc134518002)

[第三章 介质安全 5](#_Toc134518003)

[第四章 设备安全 6](#_Toc134518004)

[第五章 主机安全 8](#_Toc134518005)

[第六章 网络安全 9](#_Toc134518006)

[第七章 应用系统安全 10](#_Toc134518007)

[第八章 口令安全 13](#_Toc134518008)

[第九章 恶意代码防范 14](#_Toc134518009)

[第十章 数据备份与恢复管理 15](#_Toc134518010)

[第十一章 附则 19](#_Toc134518011)

# 环境安全

1. 机房环境
2. 机房应建设在永久性建筑中，并应远离产生粉尘、油烟、有害气体以及生产或贮存具有腐蚀性、易燃、易爆物品的场所。
3. 机房不应靠近卫生间、水房等潮湿区域，应远离强振源和强噪声源，并应避开强电磁场干扰。
4. 机房内应配备UPS不间断电源，UPS电源容量应不小于设备额定功率总和的120%，且其电池所提供的后备时间应能满足断电后设备正常关机所需的时间，一般不应小于15〜30分钟。
5. 机房内装修应使用不燃或阻燃材料，且所用材料在高温下不应释放有毒有害气体。
6. 机房内应安装烟雾及温度传感器，当出现烟雾或温度异常时应能自动报警。
7. 机房内应配备手提式（推车式）干粉灭火器或二氧化碳灭火器，对符合条件的机房也可考虑安装浸没式气体自动灭火系统。
8. 机房内应尽量安装专用空调系统， 空调系统的制冷量应与机房内各种设备的耗电量相匹配。
9. 机房内温湿度控制应满足下列要求：
10. 机柜进风区域温度：18℃至27℃
11. 机柜进风区域相对湿度：不宜大于60%
12. 机柜进风区域露点温度：5.5℃至15℃
13. 机房环境温度（停机时）：5℃至45℃
14. 机房环境相对湿度（停机时）：8%至80%
15. 机房环境露点温度（停机时）：不宜大于27℃
16. 机房内应安装测量装置，监控机房内的实时温湿度。
17. 对有条件的机房，可以安装视频监控系统，对机房内各种人员活动录像存档。
18. 机房照明设施应安全可靠，应配备应急灯及紧急出口指示灯。照明系统可部分或全部由UPS供电，以保证断电期间系统维护，此时应适当增加UPS系统容量。
19. 机房人员准入
20. 机房入口应采取适当措施，控制人员进出机房。可采用刷卡、密码、指纹、面部识别等方法进行身份认证，记录并保存人员进入机房的日志信息。
21. 应准确记录非机房管理员进出机房的日期、时间、事由、批准人等事项，非本单位人员还需记录本单位工作联系人及陪同人员。
22. 非本单位人员进入机房应得到机房管理员批准，并由机房管理员本人或委托本单位人员全程陪同。
23. 任何人不得携带任何易燃、易爆、腐蚀性、强电磁、辐射性、流体物质等对设备正常运行构成威胁的物品进入机房。
24. 机房设备进出
25. 应详细记录各类设备的进出情况，记录内容应包括设备名称、编号、功能、（原）安装位置、安装/拆除日期、操作人、批准人等信息。
26. 设备进入机房后，应根据机房管理员的安排进行安装、加电、连网，任何人不得擅自接入设备。
27. 机房管理员应为每台设备建立标签，标明设备的名称、编号、功能、负责人等主要信息。
28. 设备计划移出机房时，应根据机房管理员的安排下电、断网、拆除，任何人不得擅自移出设备。
29. 机房日常维护
30. 机房不得作为储藏室用来存放与系统运行无关的物品，不得存放各类易燃易爆物品。机房管理员有责任保持机房内整齐干净。
31. 机房管理员应定期巡查机房内各类设备的运行情况，发现问题应及时处理。
32. 机房管理员应定期检查UPS后备电池的性能参数（检查周期原则上不大于两个月）。如果发现电池参数异常，应及时更换。电池更换时应整组进行，不应单独更换个别电池。
33. 机房管理员应定期检查各类消防设施，对过期或失效灭火器应及时更换。
34. 机房管理员应定期检查空调系统运行状态，并对室内机滤网和室外机散热器进行清扫或更换。
35. 机房管理员应定期检查机房照明系统工作情况，发现问题及时修复。
36. 机房应急处理
37. 当机房供电发生故障时，机房管理员应协助设备负责人，尽快以正常方式关闭设备，以防因为UPS电池耗尽后设备掉电，造成设备损坏或数据丢失。
38. 当机房内温度传感器报警时，机房管理员应尽快到达现场，检查温度异常的原因并进行相应处置。如果发现空调系统运行不正常，应及时通知运维人员前来维修。
39. 当机房内烟雾传感器报警时，机房管理员应立刻到达现场，检查原因并进行相应处置。如确系发生火情，请按发生火灾时的应急预案处理。
40. 办公环境安全
41. 应加强对办公环境的安全管理，提高员工日常工作中的安全意识，严格控制办公环境的访问，未经领导同意，外部人员不得配备各办公区钥匙。
42. 下班前必须关闭办公室内的用电设备（包括电脑、饮水机、打印机和复印机等一切用电设备），连续放假二天及以上时，放假前必须关闭办公室总电源,办公室无人时注意关锁门窗。
43. 个人电脑需安装杀毒软件，在网络下载资源以及接受文件后进行病毒查杀，避免遭受病毒或者木马的攻击；离开座位时计算机要锁屏，桌面上不能有内部敏感信息文档；员工下班后应将重要文件、贵重物品和仪器放在抽屉或柜子内并加锁。
44. 办公室内的复印机、传真机、打印机使用后产生的内部废弃文件不得堆积，应及时取走并销毁，不可留做二次用纸,打印机、和数码照相机在使用后，如有敏感信息要及时清除，以防止被他人盗取信息；
45. 重大项目（销售、合作）的洽谈应当在内部会议室进行，避免在办公区接待来访人员。

# 信息资产管理

1. 信息资产识别
2. 信息资产是指XXX拥有和控制的电子信息和数据，以及存储、传输和处理电子信息和数据的软件、硬件及相关电力、通讯等信息技术设备设施。
3. XXX应建立和维护各信息资产清单，实现统一的资产管理台账，明确硬件资产使用责任部门、责任人和使用范围，并定期进行资产清点，对信息资产台账信息进行审核。
4. 信息系统各个相关部门分别负责维护相关信息资产，XXX负责网络及相关基础环境资产的管理与维护，业务使用部门负责业务系统相关资产的管理与维护，其他信息资产由XXX统一管理与维护，对于重要信息资产应当进行信息资产分类，如硬件资产、软件资产和数据资产等。
5. 信息资产根据其重要程度不同，分成重要信息资产和一般信息资产，各责任部门建立的信息资产清单应明确标识信息资产的重要程度，并在XXX备案。
6. 信息资产管理
7. XXX应建立统一的资产管理台账，明确资产使用责任部门、责任人和使用范围，并定期进行资产清点检查，对资产台账信息进行审核。
8. 信息资产使用人在使用过程中应确保硬件配置的完整性，不得私自更换硬件资产以及相关配件。
9. 对于需要维修的硬件资产，由设备责任人提出申请，经XXX领导批准后，把硬件资产交到维护单位进行维修。
10. 存储内部信息的信息资产在重用、维修和报废前，应确保所有存储的敏感数据或授权软件已经被移除或安全重写，并做好备份工作，确保信息不泄密、保持信息的完整性和可用性。
11. 需要报废的信息资产如含有敏感信息，应由使用部门提出申请，经XXX领导批准后，由XXX统一进行报废处理。
12. 软件资产责任人应加强对于应用软件保存、标识、安装、卸载和升级的统一管理；对于需要维修的软件资产，软件资产责任人须和XXX沟通后，由软件供货商进行维护、修改和升级，并在过程中做好安全控制。

# 介质安全

1. 介质标识
2. 存储介质是指记录存储数据的设备，主要包括磁带、磁盘、光盘、闪存、硬盘、U盘等，存储介质保存环境应保证具有足够的防火、电力、空调、湿度及其他保护措施。
3. 存储介质应分类标识，磁带、磁盘及其它存储介质等有不同的分类标签，并区分原件与拷贝件，存储介质标识必须贴在表面容易看到的地方；用于数据存储、备份或灾难恢复的存储介质应存放在一定安全级别的区域，当无人看管时，要将这些介质存放在保密柜中。
4. 对含有敏感信息的存储介质，每件表面均需要注明质量和当前件所排的序号，妥善保管，并控制授权范围，不允许将含有敏感信息存储介质和非敏感信息存储介质混放在一起。
5. 信息系统相关各部门应对介质进行登记管理，并定期对介质目录清单进行盘点。
6. 介质访问
7. 各类介质管理的责任人负责对介质的访问进行控制，对磁带、磁盘和文档库等介质的访问必须做严格限制。
8. 安装和使用存储设备时必须防止非授权的访问。
9. 所有含有内部信息的存储介质对外部人员都是保密的，严禁员工、合作方或其他人员带走。
10. 介质数据安全
11. 要介质中的数据和软件应采取加密存储。
12. 存储介质上删除敏感信息后，必须执行重复写操作防止数据恢复；任何包含敏感信息的中间存储介质，都需要销毁其中信息。
13. 当介质损坏需要送出维修或销毁时，应首先清除其中的敏感数据，以防止内部信息的非法泄漏。
14. 如果将存储介质给第三方使用，需要各部门领导确认敏感信息已经删除。
15. 介质销毁
16. 应对存储介质的销毁做统一管理，并由XXX做集中报废处置。
17. 对含有敏感信息的存储介质不再使用时，应与安全工作人员联系，销毁这些敏感信息存储介质。
18. 含有硬拷贝形式的敏感信息存储介质的报废处理方式为切碎或者烧毁。

# 设备安全

1. 设备管理
2. 所有硬件设备采购、变更、废弃时，必须首先在资产清单进行记录和描述。
3. 设备在到货验收或配置之后，必须由XXX做出相应的标识，直接体现在设备上醒目的位置，标识应包括以下内容：设备编号、设备使用部门、设备名称、设备用途、设备IP信息、设备供货商及联系方式。
4. 设备存放与使用
5. 设备的存贮与发放应严格管理，机房设备由XXX负责登记；
6. 处理核心数据信息的小型机、服务器、交换机、路由器、安全设备等重要设备应当放置在专用的带锁的机柜中。
7. 机房设备一般不得外借，因工作原因确需外借时，须经XXX批准，归还时应检验设备是否完好，设备有转移要及时做好固定资产转移手续。
8. 设备访问控制
9. 信息处理设施应根据其重要程度不同，设置不同的访问控制权限，仅允许对于设备的必要访问；
10. 存放处理核心数据信息的小型机、服务器、交换机、路由器、安全设备等重要设备应当减少对其设备直接物理访问，并确保周边物理环境的安全性，同时采取安全监控措施，包括对门禁系统的监视，必要时，对已授权的内部访问进行监视；
11. 未经批准，严禁在机房内擅自对设备进行操作，包括：
12. 关闭、启动、更换路由器、交换机、服务器以及网络安全设备等；
13. 调整和更改网络系统、网络设备、服务器、操作系统的配置参数；
14. 添加、更换和拆卸硬件设备；
15. 增加、撤除和调整网络设备和服务器的网络跳线和电源线；
16. 安装、下载、使用各种扫描、攻击、探测、侦听等安全类和黑客类软件；
17. 在域控制器上生成域用户名，在成员或独立服务器上生成服务器本机用户名；
18. 调整机房内报警、空调、通风系统参数。
19. 设备维护
20. 信息系统所有硬件设备均应指定维护管理人员，由管理人员负责对所辖设备建立日常维护工作计划，并根据供应商推荐的服务时间间隔对设备进行检查、监控和维护；
21. 设备维护工作应按照各类设备的日常维护安全操作规程进行操作，控制关键设备（包括备份和冗余设备）的启动、停止、加电和断电等操作；
22. 要注意保存维修申请记录，包括所有可疑和实际的故障记录，以及预防和维护过程中的记录；
23. 设备需要断电、停机检查时，应向相关部门主管领导申请，首先保存并备份设备中的数据和配置，方可执行断电操作，并做详细记录，影响多个核心业务系统运行的加电、断电操作应由XXX领导进行审批，批准后方可操作；
24. 建立设备维护档案，详细记录设备的基本情况（包括升级、更新情况等）、故障现象、故障分析、维修过程、处理结果等内容。

# 主机安全

1. 安全策略与配置
2. 由信息系统管理员根据业务需求和系统安全分析制定主机系统的访问控制策略，控制分配信息系统、文件及服务的访问权限。
3. 由安全管理员组织定期对系统进行漏洞扫描，并形成漏洞扫描报告，内容包含系统存在的漏洞、严重级别等方面。安全管理员及时通知系统管理员修补发现的安全漏洞，并通报处理结果。
4. 系统安全配置由系统管理员负责，在安全管理员指导下完成，其余任何人不得随意更改配置。
5. 系统管理员应对服务器安装防火墙或杀毒软件，定期对服务器系统、杀毒软件等进行升级和更新，并进行病毒清查，禁止下载和使用未经测试和来历不明的软件，禁止随意使用U盘等移动存储介质。
6. 应保留安全配置更改记录，由安全审计员负责审计。
7. 任何人员不得制造或故意输入、传播计算机病毒和其他有害数据，不得利用非法手段复制、截收、篡改计算机信息系统中数据。
8. 补丁管理
9. 应根据《漏洞和安全管理规定》中对漏洞和补丁管理的相关要求，开展漏洞修复、补丁升级测试、数据备份、补丁更新操作。
10. 主机系统批量补丁升级，应先完成补丁测试；经信息系统管理员确认未发现问题后，根据漏洞威胁的紧急程度，制定补丁分发计划，根据实际情况在生产系统中分批安装。
11. 安全管理员应督促本单位办公环境计算机安装安全补丁。
12. 账号安全
13. 主机系统管理员负责该主机操作系统用户账号的申请、删除、禁用、口令重置以及权限复审等操作，并在系统中保存操作记录。
14. 系统管理员每半年对操作系统用户账号使用情况进行一次检查，及时禁用、删除系统中的空账号、临时账号等存在安全隐患的账号。
15. 系统管理员每年对操作系统用户账号权限进行一次检查，根据用户的安全责任和工作要求对其身份以及相应的权限进行变更。
16. 做好对特殊用户和用户组的管理，包括超级用户、访客用户、匿名用户以及缺省帐户的安全管理。
17. 日志管理
18. 系统管理员对系统进行维护，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。
19. 安全审计员定期对运行日志和审计结果进行分析，并形成分析报告，报告内容包括帐户的连续多次登录失败、访问受限系统或文件的失败尝试、系统错误异常事件。

# 网络安全

1. 网络运行管理
2. 网络管理员应保持拓扑结构图与现行网络运行环境的一致性，拓扑图上包含信息应包括网络设备、安全设备的型号、名称以及与链路的链接情况等信息；
3. 通过必要的安全技术措施对网络信息进行统一管理，包括信息资产管理、网络拓扑管理、信息资源管理、网络异常流量管理、安全事件监控管理、安全策略管理、安全预警管理等网络信息；
4. 网络管理员应监控网络的运行状况，发现影响较大的网络故障时，应协调处理并及时上报；
5. 网络设备及安全设备中的运行配置文件和启动配置文件应该随时保持一致，网络设备及安全设备的日志应转发到审计系统保存，保存至少半年内的相关安全日志；
6. 定期对网络设备和安全设备进行安全检查和扫描，及时发现安全隐患，升级设备修复安全漏洞。
7. 网络安全监控
8. 网络管理员应加强网络安全监控管理，监测项目包括通信线路状态、网络设备运行状况、网络流量、网络基础服务等，及时检查网络安全隐患，发现安全事件；
9. 应对网络区域中的非法访问部署检测和审计措施，能够做到安全事件可监控、可追踪和可审计，形成安全审计报告，及时发现安全隐患，调整安全策略消除安全风险；
10. 应建立全面的安全监控中心，对信息资产的运行状态、安全状态、告警信息等进行集中管理，关联分析。

# 应用系统安全

1. 应用系统安全原则
2. 应用系统的安全管理工作应根据“谁主管谁负责、谁运维谁负责、谁使用谁负责”的原则，各个部门按照应用系统安全管理规定开展应用系统安全管理工作。
3. 应用系统运维管理应遵照以下安全原则：
4. 最小权限原则：指系统只能授予应用程序和用户必要的权限，而不能授予额外的权限；
5. 最少服务原则：指在保证系统和应用运行正常的前提下，关闭其它无关的系统服务和网络服务。
6. 用户权限管理
7. 各类系统应分别建立系统管理、安全管理和安全审计三类管理用户，并依据“权限分离”的原则分配相应的管理权限，各类管理人员只能进行职责权限下的管理维护操作，不得越权访问。
8. 为各类用户分配的权限以满足其所在岗位最低工作要求为准。
9. 应用系统安全管理员应定期检查用户的账号及其权限，及时根据用户的安全责任和工作要求对用户身份和相应的权限进行变更。
10. 系统运行管理
11. 应依据应用系统操作手册对系统进行维护，严禁进行未经授权的操作，安装各类应用软件时遵从最小化安装原则，关闭和卸载与业务运行无关的功能和服务。
12. 针对数据库数据的读取、修改、查询，由申请人向业务部门领导提交申请，经业务部门领导审批通过后，数据库管理员方可对数据库进行操作。操作结束后，数据库管理员通过邮件向业务部门负责人说明处理细节及处理结果。
13. 信息系统安全管理员应每季度进行漏洞扫描，以及时发现系统漏洞，扫描完毕后，应会同应用系统管理员分析扫描结果，然后针对扫描分析结果进行适当的处置，对高风险的漏洞及时修补。
14. 补丁管理就是通过技术和管理两种手段，对应用系统软件进行安全补丁的管理与维护，从而保证系统的即时安全性，具体实现方式包括以下几点：
15. 应及时跟进各产品的安全漏洞信息和产品厂商发布的安全补丁信息；
16. 根据漏洞的严重程度补丁分为三个级别：紧急补丁、重要补丁和一般补丁；紧急补丁必须在15天内完成加载，重要补丁必须在一个月内完成加载，一般补丁要求六个月内完成加载，对于不能加载补丁的情况，一定要采取其他的有效安全控制措施；
17. 必须从各产品厂商官方渠道获取安全补丁，补丁加载应制定严格的计划；补丁加载之前必须经过严格的测试，测试环境与生产环境尽可能一致，严禁未经测试直接在生产系统上加载补丁；
18. 补丁功能性测试主要测试补丁是否对安全漏洞进行了修补；补丁加载必须安排在业务比较空闲的时间进行，对补丁加载的操作过程必须按照计划严格操作，并详细记录；
19. 系统管理员对加载补丁后的系统必须按照计划和验证方案进行测试验证，确保补丁加载后不影响系统的性能，确保各项业务操作正常；
20. 信息系统安全管理员每季度向各系统管理员下发补丁升级自查表，检查系统的补丁升级情况。
21. 应用安全审计
22. 安全审计是通过对用户行为和操作、网络连接等应用审计内容进行统计分析，及时检查安全隐患，发现安全事件。
23. 为了能够发现和跟踪系统中发生的各种可疑事件，各个应用系统都需要启用安全审计功能，以日志的形式记录用户登录系统、文件访问操作、账户修改、访问连接等行为的过程和结果信息，做到发生可疑事件时有据可查。
24. 应用系统审计日志至少保留180天。
25. 系统变更管理
26. 信息系统在运行过程中产生的变更（包括系统变更、重要操作、物理访问和系统接入等事项）应由变更操作人（如网络管理员、系统管理员）进行申请，经涉及业务部门负责人签字审批后，由XXX负责人审核并提出意见，XXX领导签字审批。
27. 对于提交的变更申请获得审核审批后，应对批准的变更申请予以存档。
28. 信息系统变更执行人在执行后要测试变更结果并验证执行的成功与否，如果结果表明不成功，变更执行人应采取回退措施将变更回退至变更执行前的状态并进行测试，保证回退成功。
29. 信息系统变更过程中应注意：
30. 应评估应用系统变更是否会影响相关配套设备和网络配置的变更；
31. 应用系统部署发生变化时应与网络管理员、安全管理员相沟通，确保访问控制策略的一致性；
32. 网络配置发生变化时，应考虑是否会影响应用系统的稳定运行，如果有影响应提前沟通，制定应对措施；
33. 应考虑新的技术和措施可能存在的安全风险。
34. 应急变更属于特殊的变更申请，可以因问题紧迫取得特别批准，一般需要在变更申请批准后尽快实施完成。申请人应随后创建一份变更申请，并补充相应的测试及审批文档。

# 口令安全

1. 具有登录信息系统权限的用户必须设置用户口令或其它验证用户身份的方式，严禁不验证用户身份直接登录信息系统。
2. 信息系统用户口令持有人应保证口令的保密性，不应将口令记录在未妥善保管的笔记本以及其他纸质介质中（口令信封除外），严禁将口令放置在办公桌面或粘贴于办公桌，一旦发现或怀疑信息系统用户口令泄漏，应立即更换。
3. 任何人不得利用盗取、猜测、窥视、破解等非法手段获取他人信息系统用户口令，盗用他人访问权限，威胁信息系统安全。
4. 应该选择使用口令安全强度较高的口令，不应使用简单的代码和标记，禁止使用重复数字、生日、电话号码、字典单词等容易猜测的计算机系统用户口令。其具体要求如下：
5. 口令最小长度为8位；
6. 口令字符组成复杂度：口令由数字、大小写字母及特殊字符组成；
7. 口令历史：修改后的口令至少与前6次口令不同。
8. 口令最长有效期限建议90 天，可根据系统重要性和用户权限采取不同方式。当用户口令持有人岗位调整时，应根据其新的岗位职责，对其用户权限及口令进行相应调整。
9. 当用户口令持有人岗位调整时，应根据其新的岗位职责，对其用户权限及口令进行相应调整。
10. 信息系统必须提供用户口令更换机制，业务系统代码中不得预留用户口令。
11. 对于自动生成密码的系统，必须确保密码生成算法的可靠性和安全性以及密码生成“种子”的随机性；
12. 用户严禁向任何人公开其本人或他人的账号和密码的全部或部分，特别是拥有管理员权限或超级管理员权限的用户，严禁以任何明文格式存储账号和密码；
13. 严禁通过公共网络（例如，互联网、公共电话网等），以明文格式传送账号和密码。
14. 信息安全管理员必须设定所有用户登录尝试的次数限制，对于信息安全管理员和系统管理员账号，登录尝试次数为3次。对于其他账号，登录尝试次数为5次，一旦在一定时间内使用同一个用户账号的失败登录超过限定次数，该账号会被自动禁止，直到重新激活该用户账号；
15. 信息安全管理员在发现任何企图非法使用某用户账号的情况时，必须强制该用户更改密码。

# 恶意代码防范

1. 各信息系统应统一规划、统一部署具有国家许可的正版计算机防病毒系统软件，信息系统中所有服务器和终端必须安装配发的计算机防病毒软件，及时更新恶意代码库，否则不允许连入网络和处理工作。
2. 在使用U盘等移动存储设备或外来计算机接入网络和主机时应先进行病毒等恶意代码扫描检查。
3. 各信息系统内的所有服务器和计算机终端应使用XXX下发的正版软件，禁止随意安装软件，防止其中可能存在恶意软件；
4. 基础设施安全管理员对防病毒软件系统进行监控，记录病毒查杀情况；
5. 各信息系统内的服务器、桌面计算机及便携式计算机一旦发现被计算机病毒感染，应先将计算机与网络隔离，确保病毒库已更新至最新版本,并及时进行病毒查杀处理；当情况严重且无法在规定时限内紧急恢复或有效控制时，应及时上报启动相应应急响应预案，应注意保留防病毒系统记录；
6. 应定期执行计算机病毒检测、清除工作，检测应扫描所有的计算机硬盘分区，以发现硬盘中可能存在的病毒或异常情况，同时将检测结果进行集中保存，做为后期检查的依据。
7. 应定期组织各个部门人员进行安全培训，提高每个人的防病毒意识，并及时告知防病毒软件和恶意代码库的最新版本。

# 数据备份与恢复管理

1. 备份管理
2. 业务系统备份采取定期备份与动态备份相结合的原则。定期备份按一定周期有计划进行；动态备份是指当操作系统、应用系统发生较大变动后，实时进行的备份。操作系统和数据库数据定期进行备份，在系统变更或较大应用调整前进行一次操作系统和应用软件备份，并同时同步备份机上相关内容；对系统和应用的配置备份定期进行。
3. 业务系统管理人员需确保业务系统的所有网络设备、操作系统的系统配置数据及核心业务数据定期进行备份，备份策略正确。
4. 数据备份采用全量备份或增量备份。数据备份策略的制定应综合系统性能、存储容量、数据量增长速度、业务需求、备份方式、存储介质、存储介质型号、有效期等因素。备份策略的制定应考虑在特殊日、版本升级日增加备份。
5. 数据备份应采用性能可靠、不宜损坏的介质，如磁带、光盘等。备份数据的物理介质应注明数据的来源、备份日期、恢复步骤等信息，并置于安全环境保管。
6. 数据备份时，要仔细检查备份作业或备份程序的执行结果，核实目标备份与源备份内容一致，确保备份数据的完整性和正确性。
7. 数据备份时，应及时记录备份情况，包括备份作业，备份周期、时间、内容、数据保存期限，介质型号、介质容量、业务种类、转存情况、异地备份记录、相关变更记录等信息，并进行当日备份的问题记录。
8. 操作系统备份要求：
9. 操作系统层的备份范围包括操作系统和系统运行所产生的登录和操作日志文件。
10. 操作系统应每半年至少备份一次。
11. 操作系统运行所产生的登录和操作日志文件应每月至少备份一次。
12. 在操作系统安装系统补丁，进行系统升级，修改系统配置或其它可导致系统改变的情况发生前后必须进行操作系统备份。
13. 操作系统层的备份由系统管理员负责实施。
14. 所有操作系统层的备份完成后应至少保留三个月。
15. 数据库备份要求：
16. 数据库层的备份范围包括数据库的日志文件、数据文件和系统程序文件。
17. 数据库日志文件包括归档日志文件、告警日志文件和跟踪文件。
18. 在安装数据库补丁、应用系统补丁、数据库升级或其它导致数据库改变的操作发生前后必须备份完整的数据库数据文件和数据库程序文件，备份后应执行备份介质异地存放。
19. 数据库数据文件应每周至少备份一次。
20. 数据库归档日志应每天进行增量备份。
21. 当数据库发生故障时，如需进行系统恢复，应先备份故障数据库的数据文件。
22. 数据库层备份由数据库管理员负责实施。
23. 所有备份的数据库日志文件和数据库程序文件备份应至少保留三个月。
24. 应用系统备份要求：
25. 应用系统层备份包括应用系统程序文件和日志文件。
26. 应用系统程序文件和日志文件应每月至少备份一次，备份后应执行备份介质异地存放。
27. 根据补丁级别，在安装应用系统补丁前后视要求执行系统备份。
28. 应用系统备份由应用系统管理员负责实施。
29. 所有的应用系统备份应至少保留三个月。
30. 系统备份的存放和更换
31. 系统备份为一式二份，每月备份一次。
32. 如有可能把需要永久保管的备份做成光盘保存。
33. 备份具体过程及要求
34. 应用软件的备份：由业务部门自行备份，每月第一个工作日交于网管部门，并填妥备份管理表格，包括时间、提交备份人、由统一检查，填写备份结果后，入库保存。
35. 业务数据的备份：值班人员每天登录完毕后进行备份，备份结束后查看出错信息，确定备份是否正确完成，并把完成后的磁带放入保险箱中，认真填写值班记录表，统一将磁带放回磁带库中；每天早上检查日志文件查看备份是否正常完成。
36. 系统备份：对系统进行备份后，做好登记，入库保存。
37. 日志文件备份：每个月第一工作日备份一次日志。做好登记，入库保存。
38. 系统配置文件备份：备份所有服务器上的系统配置文件，做好登记入库保存。
39. 备份介质管理
40. 对备份的数据需定期进行抽检，采用将备份数据恢复到测试环境的方式对备份数据的正确性进行验证。
41. 备份管理人员应对本地备份数据情况进行每天一次的检查。
42. 为尽快恢复故障，应在本地（主场所）保留备份介质，同时为了避免主场所的灾难所导致的破坏，还应做好异地备份。异地备份场所的物理和环境保护级别不能低于主场所，主场所所采用的媒介控制措施应当扩展涵盖备用场所。
43. 备份管理人员应及时对冷备介质进行异地存放。
44. 备份管理人员应制定详细可操作的备份恢复操作方案，并由业务系统主管领导审批签字。
45. 备份管理人员根据方案每半年对本地和异地备份的业务数据在测试环境下进行一次恢复性测试，确保演练备份恢复时间在预定时间内，以及备份介质没有过期，备份数据可用、完整。
46. 备份管理人员应根据备份数据须保存最长期限的要求在备份介质使用寿命到期之前及时更换备份介质。
47. 正式的备份数据恢复以及过期的备份数据销毁必须经相关业务系统部门主管领导认可后方可进行。
48. 本地备份介质保存在本地机房中，只有本地经过授权进入机房的人员才能接触系统备份磁带。
49. 异地备份介质保存在异地专用库房中，库房钥匙（或门禁卡等）只有负责异地存放备份介质的维护人员掌握。
50. 应根据日常备份的需要提前估算并购买备份介质的数量，并及时检查备份介质的可用量，避免备份介质写满或者容量不足的情况发生。
51. 备份介质达到使用年限后，应对备份介质上保存的数据进行审核，如需继续保存，则应由备份管理员将数据装移到新的备份介质上，并做恢复性测试，并签字确认。
52. 安全管理员应每月对备份介质进行审核，并签字确认。
53. 备份恢复管理
54. 在解决故障的过程中，如需恢复生产系统中的数据库环境，必须首先提出申请，获得资料服务室负责人的批准后才可实施。
55. 数据恢复前，必须根据情况对所需要恢复的数据进行必要的备份，防止有用数据的丢失。
56. 数据恢复必须严格按照操作手册执行，出现问题时由资料服务室相关人员进行现场技术支持。
57. 数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。
58. 由数据备份人员根据不同业务系统的实际拟定需要测试的备份数据项目以及测试的周期。
59. 对于因设备故障、操作失误等造成的一般故障，需要恢复部分设备上的备份数据，遵循异常事件处理流程，由设备管理员或数据库管理员负责恢复。
60. 对于因灾难等原因造成的重大事故，遵循持续性管理流程，启动灾难恢复计划进行恢复。

# 附则

1. 本制度由XXX制定，并负责解释和修订。由XXX讨论通过，发布执行。
2. 本制度自发布之日起执行。