目录

[一、信息安全总体策略 10](#_Toc530487894)

[第一章总则 10](#_Toc530487895)

[第二章适用范围 10](#_Toc530487896)

[第三章术语定义 10](#_Toc530487897)

[第四章组织职责 10](#_Toc530487898)

[第五章管理原则 10](#_Toc530487899)

[第六章总体目标 11](#_Toc530487900)

[第七章安全框架 12](#_Toc530487901)

[第八章策略制定与维护 13](#_Toc530487902)

[第九章持续改进 13](#_Toc530487903)

[第十章附则 13](#_Toc530487904)

[二、文档体系管理规定 15](#_Toc530487905)

[第一章总则 15](#_Toc530487906)

[第二章适用范围 15](#_Toc530487907)

[第三章术语定义 15](#_Toc530487908)

[第三章职责 15](#_Toc530487909)

[第四章文件起草 15](#_Toc530487910)

[第五章文件评审 16](#_Toc530487911)

[第六章文件发布 17](#_Toc530487912)

[第七章文件修订 18](#_Toc530487913)

[第八章文件废止 18](#_Toc530487914)

[第九章持续改进 19](#_Toc530487915)

[第十章附 则 19](#_Toc530487916)

[三、管理组织架构规定 21](#_Toc530487917)

[第一章总则 21](#_Toc530487918)

[第二章适用范围 21](#_Toc530487919)

[第三章组织目标 21](#_Toc530487920)

[第四章等级保护组织架构 21](#_Toc530487921)

[第五章组织的等级保护职责略 21](#_Toc530487922)

[第六章持续改进 26](#_Toc530487923)

[第七章附则 26](#_Toc530487924)

[附录一XXX会议纪要 27](#_Toc530487925)

[附录二XXX信息安全岗位表 28](#_Toc530487926)

[四、安全检查管理规定 28](#_Toc530487927)

[第一章总则 28](#_Toc530487928)

[第二章适用范围 28](#_Toc530487929)

[第三章术语定义 28](#_Toc530487930)

[第四章组织职责 29](#_Toc530487931)

[第五章通用要求 29](#_Toc530487932)

[第六章安全检查准备 29](#_Toc530487933)

[第七章 安全检查报告 30](#_Toc530487934)

[第八章安全检查整改 30](#_Toc530487935)

[第九章检查工具的使用 30](#_Toc530487936)

[第十章持续改进 30](#_Toc530487937)

[第十一章附则 30](#_Toc530487938)

[附录一安全检查汇总表 31](#_Toc530487939)

[附录二安全检查记录表 32](#_Toc530487940)

[2.1 组织机构 34](#_Toc530487941)

[2.2 标准制度规范 34](#_Toc530487942)

[2.3 安全培训、教育 34](#_Toc530487943)

[5.1 信息系统巡检 34](#_Toc530487944)

[5.2 应急演练 34](#_Toc530487945)

[五、人力资源信息安全管理规定 36](#_Toc530487946)

[第一章总则 36](#_Toc530487947)

[第二章适用范围 36](#_Toc530487948)

[第三章术语定义 36](#_Toc530487949)

[第四章组织职责 36](#_Toc530487950)

[第五章入职信息安全管理 36](#_Toc530487951)

[第六章在职信息安全管理 38](#_Toc530487952)

[第七章调动信息安全管理 38](#_Toc530487953)

[第八章离职信息安全管理 38](#_Toc530487954)

[第九章持续改进 39](#_Toc530487955)

[第十章 附则 39](#_Toc530487956)

[附录一XXX人员安全审查记录 40](#_Toc530487957)

[附录二XXX人员录用安全考核记录表 41](#_Toc530487958)

[附录三XXX关键岗位安全协议 42](#_Toc530487959)

[六、信息安全培训和考核管理规定 44](#_Toc530487960)

[第一章总则 44](#_Toc530487961)

[第二章适用范围 44](#_Toc530487962)

[第三章术语定义 44](#_Toc530487963)

[第四章 组织职责 44](#_Toc530487964)

[第五章安全培训管理程序 44](#_Toc530487965)

[第六章安全考核管理程序 46](#_Toc530487966)

[第七章持续改进 46](#_Toc530487967)

[第八章附则 46](#_Toc530487968)

[附件一信息安全培训汇表 47](#_Toc530487969)

[附件二专业安全技术培训申请审批表 48](#_Toc530487970)

[附件三员工信息安全考核表 49](#_Toc530487971)

[附件四关键岗位考核内容表 50](#_Toc530487972)

[附件五关键岗位考核指标对应表 52](#_Toc530487973)

[附件六信息安全考核汇总表 53](#_Toc530487974)

[附件七人员培训记录表 54](#_Toc530487975)

[附件八年培训调查（计划）表 55](#_Toc530487976)

[七、信息系统等级保护建设管理规定 56](#_Toc530487977)

[第一章总则 56](#_Toc530487978)

[第二章适用范围 56](#_Toc530487979)

[第三章组织职责 56](#_Toc530487980)

[第四章系统定级 56](#_Toc530487981)

[第五章安全检查报告 58](#_Toc530487982)

[第六章系统建设 59](#_Toc530487983)

[第七章系统测评 59](#_Toc530487984)

[第八章系统终止 60](#_Toc530487985)

[第九章持续改进 60](#_Toc530487986)

[第十章附则 60](#_Toc530487987)

[附录一系统安全设计方案评审表 61](#_Toc530487988)

[附录二系统测试验收评审表 62](#_Toc530487989)

[附录三系统转移、终止或废弃申请表 63](#_Toc530487990)

[附录四系统定级专家论证文档 64](#_Toc530487991)

[附录五系统维护手册（模板） 65](#_Toc530487992)

[(一) 系统网络结构 67](#_Toc530487993)

[(二) 系统软、硬件配置 67](#_Toc530487994)

[(三) 应用软件功能结构 68](#_Toc530487995)

[(一) 备份及恢复对象 75](#_Toc530487996)

[(二) 备份模式、命令 75](#_Toc530487997)

[(三) 恢复模式、命令 76](#_Toc530487998)

[八、工作环境管理规定 77](#_Toc530487999)

[第一章总侧 77](#_Toc530488000)

[第二章适用范围 77](#_Toc530488001)

[第三章 术语定义 77](#_Toc530488002)

[第四章职责 77](#_Toc530488003)

[第五章办公区域访问控制 77](#_Toc530488004)

[第六章办公环境安全 78](#_Toc530488005)

[第七章办公用计算机安全 78](#_Toc530488006)

[第八章监督和检查 80](#_Toc530488007)

[第九章持续改进 81](#_Toc530488008)

[第十章附 则 81](#_Toc530488009)

[九、信息系统信息资产管理规定 81](#_Toc530488010)

[第一章总则 81](#_Toc530488011)

[第二章适用范围 81](#_Toc530488012)

[第三章术语定义 81](#_Toc530488013)

[第四章职责 81](#_Toc530488014)

[第五章资产分类 81](#_Toc530488015)

[第六章资产分级 82](#_Toc530488016)

[第七章信息资产标识 82](#_Toc530488017)

[第八章信息资产维护 83](#_Toc530488018)

[第九章闲置报废资产管理 83](#_Toc530488019)

[第十章持续改进 83](#_Toc530488020)

[第十一章附则 83](#_Toc530488021)

[附录一XXX XXXX 系统信息资产清单 83](#_Toc530488022)

[十、存储介质管理规定 85](#_Toc530488023)

[第一章总则 85](#_Toc530488024)

[第二章适用范围 85](#_Toc530488025)

[第三章 术语定义 85](#_Toc530488026)

[第四章组织职责 85](#_Toc530488027)

[第五章存储介质标识 85](#_Toc530488028)

[第六章存储介质访问 85](#_Toc530488029)

[第七章存储介质保管 86](#_Toc530488030)

[第八章存储介质销毁 86](#_Toc530488031)

[第九章持续改进 86](#_Toc530488032)

[第十章附则 86](#_Toc530488033)

[附录一存储介质记录 87](#_Toc530488034)

[附录二存储介质销毁申请表 87](#_Toc530488035)

[十一、设备安全配置管理规定 88](#_Toc530488036)

[第一章总则 88](#_Toc530488037)

[第二章适用范围 88](#_Toc530488038)

[第三章术语定义 88](#_Toc530488039)

[第四章组织职责 89](#_Toc530488040)

[第五章账户管理 89](#_Toc530488041)

[第六章系统密码管理 91](#_Toc530488042)

[第七章补丁管理 96](#_Toc530488043)

[第八章日志管理 97](#_Toc530488044)

[第九章备份管理 99](#_Toc530488045)

[第十章恢复管理 101](#_Toc530488046)

[第十一章持续改进 101](#_Toc530488047)

[第十二章附则 101](#_Toc530488048)

[附录一XXX业务系统临时帐户申请表 103](#_Toc530488049)

[附录二XXX业务系统帐户清单 104](#_Toc530488050)

[附录三XXX业务系统补丁安装登记表 105](#_Toc530488051)

[附录四XXX业务系统备份恢复操作方案 106](#_Toc530488052)

[附录五XXX业务系统备份恢复测试记录 107](#_Toc530488053)

[附录六XXX备份介质更换记录 108](#_Toc530488054)

[附录七XXX本地备份登记记录 109](#_Toc530488055)

[附录八本地备份介质使用记录 110](#_Toc530488056)

[附录九本地备份介质授权记录 111](#_Toc530488057)

[附录十业务系统备份数据清单 112](#_Toc530488058)

[附录十一异地备份登记记录 114](#_Toc530488059)

[附录十二异地备份介质恢复测试记录 115](#_Toc530488060)

[附录十三异地备份介质使用记录 116](#_Toc530488061)

[附录十四异地备份介质授权记录 117](#_Toc530488062)

[附录十五主机操作日志 118](#_Toc530488063)

[十二、防病毒管理规定 119](#_Toc530488064)

[第一章总则 119](#_Toc530488065)

[第二章适用范围 119](#_Toc530488066)

[第三章术语定义 119](#_Toc530488067)

[第四章组织职责 119](#_Toc530488068)

[第五章防病毒管理内容 120](#_Toc530488069)

[第六章防病毒应用规定 121](#_Toc530488070)

[第七章惩罚制度 121](#_Toc530488071)

[第八章持续改进 121](#_Toc530488072)

[第九章附则 121](#_Toc530488073)

[附录一人工查杀病毒记录 122](#_Toc530488074)

[十三、沟通与合作 123](#_Toc530488075)

[第一章总则 123](#_Toc530488076)

[第二章适用范围 123](#_Toc530488077)

[第三章组织职责 123](#_Toc530488078)

[第四章附则 124](#_Toc530488079)

[十四、外来人员管理制度 124](#_Toc530488080)

[第一章总则 124](#_Toc530488081)

[第二章适用范围 125](#_Toc530488082)

[第三章附则 125](#_Toc530488083)

[十五、变更管理制度 126](#_Toc530488084)

[第一章总则 126](#_Toc530488085)

[第二章变更定义 126](#_Toc530488086)

[第三章职责分工 127](#_Toc530488087)

[第四章 系统变更流程 127](#_Toc530488088)

[系统变更方案 128](#_Toc530488089)

[新增服务器 128](#_Toc530488090)

[服务器迁移 129](#_Toc530488091)

[新建应用系统 129](#_Toc530488092)

[应用软件变更 130](#_Toc530488093)

[第五章附 则 130](#_Toc530488094)

[十六、信息系统建设管理 132](#_Toc530488095)

[第一章采购和安装 132](#_Toc530488096)

[（一）软件的采购和安装 132](#_Toc530488097)

[（二）设备的采购和安装 133](#_Toc530488098)

[第二章软件开发管理（外包软件开发管理） 133](#_Toc530488099)

[第三章工程实施 134](#_Toc530488100)

[第四章测试验收 134](#_Toc530488101)

[第五章系统交付 135](#_Toc530488102)

[十七、系统运维管理规定 135](#_Toc530488103)

[第一章 基本要求 135](#_Toc530488104)

[第一节 总则 135](#_Toc530488105)

[第二节 组织架构及岗位职责 136](#_Toc530488106)

[第三节 管理规程和技术规范 137](#_Toc530488107)

[第四节 软硬件设备管理 137](#_Toc530488108)

[第五节 运维工作督促和检查 138](#_Toc530488109)

[第二章 运行保障 138](#_Toc530488110)

[第一节 机房管理 138](#_Toc530488111)

[第二节 值班管理 139](#_Toc530488112)

[第三节 日常操作 139](#_Toc530488113)

[第四节 监控分析 140](#_Toc530488114)

[第五节 网络管理 140](#_Toc530488115)

[第六节 系统管理 144](#_Toc530488116)

[第七节 数据库管理 147](#_Toc530488117)

[第八节 应用系统运维 148](#_Toc530488118)

[第九节 数据与介质管理 148](#_Toc530488119)

[第十节 事件与问题管理 150](#_Toc530488120)

[第三章 系统维护 151](#_Toc530488121)

[第一节 交付与测试 151](#_Toc530488122)

[第二节 系统变更 152](#_Toc530488123)

[第三节 配置管理 153](#_Toc530488124)

[第四章 监控室管理 153](#_Toc530488125)

[第一节 出入管理 153](#_Toc530488126)

[第二节 终端与介质管理 154](#_Toc530488127)

[第三节 堡垒机与授权管理 154](#_Toc530488128)

序言

信息安全等级保护是国家在国民经济和社会信息化的发展过程中，提高信息安全保障能力和水平，维护国家安全、社会稳定和公共利益，保障和促进信息化健康发展的基本策略。信息化发展的不同阶段和不同的信息系统有着不同的安全需求，必须从实际出发，综合平衡安全成本和风险，优化信息安全资源的配置，确保重点。要重点保护基础信息网络和关系国家安全、经济命脉、社会稳定等方面的重要信息系统。为满足XXX（简称“XXX”）信息化建设符合信息安全管理规范，特建立本信息安全等级保护管理体系，并在全医院执行。

# 一、信息安全总体策略

## 第一章总则

第一条 为了加强信息系统的信息安全管理，明确XXX信息系统信息安全管理的总的目标和方向，保护医院所有的信息资产，积极预防安全事件的发生，安全事件的影响最小化，以确保业务的持续性，特制定本策略文件。

## 第二章适用范围

第二条 本策略文件适用于XXX信息系统系统维护管理人员、使用人员、网络、服务器、终端设备、信息系统的专用设备、物理环境，以及有关的数据、文档等。

## 第三章术语定义

第三条 安全策略：是纲领性的安全策略主文档，描述XXX医院信息系统业务安全目标和管理层意图、支持目标和指导原则，是信息安全实践的根本性和指导性的文件。

## 第四章组织职责

第四条 信息安全等级保护工作领导小组（以下简称等级保护领导小组）负责审批信息安全策略文件；负责对XXX信息系统信息安全方面的指导方向、安全建设等重大事项做出决策，解决各个部门之间安全协同工作的协调问题，支持和推动信息安全工作在整个XXX范围内的实施。

第五条 信息安全等级保护工作工作小组（以下简称等级保护工作小组）负责具体执行安全管理策略文件的建立、实施、运作、监控、评审、维护和改进工作。

第六条 XXX所有员工有责任了解自身在信息系统信息安全方面的责任并认真执行。

## 第五章管理原则

第七条 信息安全管理工作实行“积极防范、突出重点、职责到位、保障业务”和“谁主管、谁负责”的管理原则。

## 第六章总体目标

第八条 遵守国家相关法律法规，结合XXX实际情况，依据现有管理和文化体系，逐步建设一套适用于XXX的信息安全管理体系，实现XXX对社会的公开承诺，并满足XXX不断发展的业务需求。

## 第七章安全框架

第九条 安全管理制度

⑴建设并完善由安全策略、管理制度、操作规程组成的信息安全管理体系。

⑵信息安全策略文件须由等级保护领导小组审核批准，并公布与传达给XXX范围内所有人员与相关外部团体。信息安全策略文件在规划期间内或有重大变更发生时需通过等级保护领导小组的审查及修订。

第十条 安全管理机构

⑴建立信息安全管理组织，以满足信息安全管理体系持续运行的目标。

⑵ 加强与外部团体的沟通和合作，及时获取相关信息。

⑶ 建立安全检查制度，定期对信息系统进行安全检查。

第十一条 人员安全

⑴加强人员录用和离岗过程的安全管理，并定期对所有人员进行安全培训和考核，加强安全意识。

⑵对所有操作或访问信息资产第三方团体，必须向其阐明相关的责任，并明确告知其有责任恰当地使用和保护这些信息资产。

第十二条系统建设

⑴系统建设初期必须根据系统定级情况进行安全方案设计，对可行性进行论证。

⑵确保安全和密码产品采购和使用符合国家的有关规定；并选择具备资质的安全服务商。

⑶确保在系统的开发与维护过程中，相关的安全功能和需求已被嵌入到系统内。在开发新系统时，安全功能应包含在初始的系统分析与需求描述中。这些描述必须包括自动的和手动的安全控制。这些控制必须通过测试，而且能够整合到正在运行的环境中。

第十三条 系统运维

⑴需在信息系统及其相关的设备在物理上实施保护，防止偷窃、滥用、损坏或未经授权的访问。

⑵需对信息系统相关的信息资产进行适当保护, 所有信息资产必须有确定的属主并且根据其敏感度进行分类和控制。

⑶所有信息系统必须制定相应的操作规范，通过对日常操作的管理、介质的管理、恶意代码防范控制确保信息系统范围内信息处理设施的正确和安全操作。

⑷对三级系统应建立安全管理技术平台，对信息资产安全事件实现监控和响应。

⑸所有信息系统变更应有审批流程，并有完善的恢复流程。

⑹建立有效的安全事件响应和处理机制，安全事件必须及时的发现、报告、处理、调查、上报并修正，并且有事后的总结，以吸取经验教训，避免以后再发生同类型的事件，把XXX的损失降到最小。

⑺建立完善的应急预案，以确保事故发生时，对业务活动的影响降至最小。

## 第八章策略制定与维护

第十四条 信息安全策略文件由技术中心安全管理员编写，经等级保护领导小组批准后，向所有相关部门、第三方机构和相关人员发布。

第十五条 等级保护领导小组监督信息安全活动，是否与策略的目标一致，达到策略的要求。

第十六条 等级保护领导小组审查和处理违反安全策略的行为。

第十七条 等级保护工作小组定期对信息安全策略进行

总结和评审（附件一、评审记录表），确保策略的有效性和可操作性。

## 第九章持续改进

第十八条 为了保证本策略文件的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章附则

第十九条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第二十条 本文件自发布之日起执行。

|  |  |  |
| --- | --- | --- |
| 会议名称 |  | |
| 主要人员 |  | |
|  | | |
| 评审意见： | | 审批结果： |

日期：

年

月

日

附件一、安全管理制度评审记录表

评审记录表

# 二、文档体系管理规定

## 第一章总则

第一条 为保证XXX等级保护管理体系的持续性、时效性以及适应性，满足业务不断变化的安全管理的需要，明确等级保护管理体系的制定、发布、评审和修订过程中管理职责，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX等级保护管理体系制定和发布过程。

## 第三章术语定义

第三条 信息安全等级保护管理体系是指依据国家信息安全等级保护的要求建立的系统内进行信息安全管理的制度、方针、策略、流程、指南、记录等管理方面的规章制度集合。

## 第三章职责

第四条 信息安全等级保护工作领导小组的职责见《XXX等级保护管理组织架构规定》的要求。

第五条 信息安全等级保护工作工作小组的职责见《XXX等级保护管理组织架构规定》的要求。

第六条 相关人员，是指我院等级保护管理体系涉及的人员。包括但不限于：系统管理员、网络管理员、数据管理员和安全管理员等，其职责见《XXX等级保护管理组织架构规定》的要求。

## 第四章文件起草

第七条 XXX信息安全管理体系规范文件由技术中心或者信息安全等级保护工作工作小组负责起草或组织起草。

第八条 负责起草的部门应当确定一名熟悉相关内容员工为项目负责人， 如涉及多个部门时，可由有关部门共同派人组成联合起草小组，由主要起草部门负责牵头组织。

第九条 起草的规范性文件应当结构严谨、内容完备、形式规范、条理清楚、用词准确、文字简洁。

第十条 应当明确规定如下内容：

⑴制定的目的和依据；

⑵适用范围；

⑶术语定义；

⑷组织职责；

⑸具体管理要求或规定；

⑹必要的附则；

⑺与规范内容相关的资料性附录和参考性附录。

第十一条 报送审查的管理制度送审稿应当由起草部门负责人签署后报信息安全等级保护工作领导小组审查。几个部门共同起草的规范送审稿，应当由起草部门负责人共同签署后报信息安全等级保护工作领导小组审查。

第十二条 下列材料应当与规范送审稿一并报送信息安全等级保护领导小组审查：

⑴起草说明；

⑵与此规范内容有关的规范性文件；

⑶汇总的各方意见；

⑷如需制定实施细则，应当提交实施细则的主要内容和实施细则拟出台的时间；

⑸其它需要报送的材料。

第十三条 信息安全等级保护工作领导小组主要从以下方面对送审稿进行审查：

⑴是否符合权限和程序；

⑵是否符合原则；

⑶是否与其它规范相协调、衔接；

⑷是否已对有关不同意见进行协调；

⑸是否具有可行性；

⑹是否符合相关技术要求⑺需要审查的其他内容。

第十四条 由信息安全等级保护工作领导小组对送审稿提出审查结论，对草案涉及的有关争议问题以及修改情况作重点说明。由信息安全等级保护工作领导小组负责人签署的书面审查报告应当反馈起草部门。

## 第五章文件评审

第十五条 XXX信息安全等级保护工作工作小组定期（至少每年一次）开展等级保护管理体系的评审工作，以确保整个等级保护管理体系的充分性、适当性和有效性。

第十六条 等级保护管理体系评审内容：

⑴根据业务系统的性质和安全要求，确定（或复审）等级保护管理体系的范围，建立（复审）等级保护管理体系，包括信息安全策略、标准和程序；

⑵对等级保护管理体系审核结果进行评审，分析导致不符合项的原因；

⑶审查审核对象的反馈信息；

⑷总结已发现的安全事件和漏洞；

⑸审查现行的安全控制措施和相关技术是否有效；

⑹复查修订措施的实施状况；

⑺检查先前管理评审中所定义的措施的实施状况；

⑻审查改善措施的建议；

⑼复查业务和法律法规方面的变更（包括但不限于：业

务需求、客户需求的变更和新颁布的法律法规）；

⑽ 审查可能影响等级保护管理体系的任何变更；

⑾为协调相关信息安全的实施，评审相关资源的充足性。

第十七条 评审工作必须至少每年举行一次，发生以下情况时，也需要启动管理评审工作：

⑴系统业务发生重大变更；

⑵系统信息安全策略的重大变更；

⑶目前等级保护管理体系的执行不力；

⑷系统等级保护管理体系的范围发生变更；

⑸相关标准法规发布修订版本或有变更；

⑹评审工作的会议记录均需归档，以保存正式的记录。

## 第六章文件发布

第十八条 规范草案经信息安全等级保护工作领导小组审议并原则通过后，起草部门根据审议中提出的修改意见对草案进行修改，经信息安全等级保护工作领导小组负责人签发,以XXX管理制度规范形式公布。

第十九条 文件的发布应遵照统一的格式，进行版本控制；并应注明发布范围，对收发文进行登记。对发布的制度应在《附录一、中医医院信息安全等级保护管理制度发布记录表》中进行记录。

## 第七章文件修订

第二十条 采取修订措施可能由以下原因，包括但不限于：

⑴来自系统等级保护管理体系相关人员的反馈信息或调查申请；

⑵ 信息安全管理评审的会议讨论中发现的问题；

⑶ 等级保护管理体系的审核发现的不符合项。

第二十一条 调查问题的起因：

⑴由信息安全等级保护工作工作小组指派专门的人员负责对问题进行分析调查并确认问题的起因；

⑵调查人员需提供尽可能多的关于整个问题调查的详细结果。作为修订措施报告的一部分，也可以提供一些额外的补充信息。

第二十二条 执行修订措施：

⑴基于所调查出的问题起因，经确认后采取以下措施，包括但不限于：

①准备制定或更新相关管理程序；

②培训/通知相关人员知晓。

⑵执行人员负责跟踪所执行修订措施的效果，以判断所实施的修订措施是可证实和可验证的。

第二十三条 措施的验证：

⑴如果验证出所采取的措施达到预期效果，说明修订措施成功，应该结束跟踪。验证阶段包括以下两个部分：

①对所规定修订措施的执行程度进行验证；

②对修订措施的执行效果进行验证。

⑵措施验证的结果必须有详细的说明，且对相关记录进行保存。

## 第八章文件废止

第二十四条 遇有下列情形之一的，管理制度应当及时废止：

⑴因有关主管部门行政法规废止或者修改，失去制定依据或者没有必要继续执行的；

⑵因规定的事项已执行完毕或者因实际情况变化，没有必要继续执行的；

⑶新的管理制度已取代了旧的管理制度的；

⑷其它应当予以废止的情况。

第二十五条 对需要废止的管理制度由信息安全等级保护工作领导小组明文废止或者宣布失效。

第二十六条 对新制定的规范可以替代旧的规范的，应当在新的规范中列出详细目录，明文废止被替代的规范。

## 第九章持续改进

第二十七条 为了保证本文件的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章附 则

第二十八条 XXX技术中心起草信息安全等级保护管理制度参照本办法规定办理。

第二十九条 对于违反本办法制定的规范性文件，信息安全等级保护工作领导小组可责令限期改正、对有关规范性文件予以撤销。

第三十条 本规定自发布之日起执行。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 管理制度名称 | 制订者 | 发布者 | 生效时间 | 版本 | 分发范围 | 失效时间 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

附录一、信息安全等级保护管理制度发布记录表

# 三、管理组织架构规定

## 第一章总则

第一条 为加强XXX等级保护工作的组织协调，建立健全等级保护管理制度和运行机制，切实提高广州中医医院等级保护工作水平，制定本规范。

## 第二章适用范围

第二条 本文件适用于XXX。

## 第三章组织目标

第三条 本规范旨在实现等级保护组织的以下目标：

⑴管理组织内的信息安全等级保护工作；

⑵保障外部组织访问组织内信息资产的安全。

## 第四章等级保护组织架构

第四条 为加强对XXX信息安全等级保护工作的领导，XXX设立信息安全等级保护工作领导小组（以下简称等级保护领导小组）和信息安全等级保护工作工作小组（以下简称等级保护工作小组）。在技术中心设立安全管理员、安全审计员、数据库管理员、网络管理员和系统管理员等专职岗位。

第五条 本部各部门作为等级保护工作的具体执行单位，其主要负责人为本单位信息安全等级保护工作的第一责任人，并指定一名信息安全管理员作为等级保护工作联络员，负责本单位内的有关信息安全等级保护工作。

第六条 为了保证等级保护管理工作的有效性，稽查部作为独立的常设机构，接受XXX办公室下达的审计任务，负责等级保护管理体系审核工作，在等级保护工作小组的协助下，进行定期审计或专项审计，并向XXX办公室提交报告。

## 第五章组织的等级保护职责略

第七条 信息安全等级保护工作领导小组的职责包括：

⑴根据公安部的总体要求，结合XXX的实际情况，统一领导XXX信息安全等级保护的相关工作；

⑵负责与国家等级保护主管机构、上级主管部门的沟通和交流，组织落实广州市公安局关于信息安全等级保护工作的方针、政策和各项重大部署；负责有关等级保护工作的落实和推行，并负责报告XXX有关等级保护状况和重要事件；

⑶负责协调XXX内部等级保护工作，分配等级保护管理目标、职责，并支持和推动等级保护工作在XXX范围内的实施；

⑷负责对与等级保护管理有关的重大事项进行决策，包括安全组织机构调整、以及等级保护管理重大策略变更；

⑸审定和发布XXX信息安全的发展战略、总体规划、重大政策、管理规范和技术标准；

⑹ 评审与监督重大信息安全事故的处理；

第八条 信息安全等级保护工作工作小组的职责包括：

⑴直接对信息安全等级保护工作领导小组负责，承担等级保护的具体工作，协助等级保护工作领导小组在等级保护事务上的决策；

⑵负责等级保护政策的贯彻与落实，并协调各等级保护执行单位以及与外部组织间有关的等级保护工作；

⑶负责等级保护管理体系的建立、实施和日常运行，起草等级保护政策，确定等级保护管理标准，督促各等级保护执行单位对于等级保护政策、措施的实施；

⑷负责对员工的等级保护工作意识教育和安全技能培训；

⑸负责维护安全事件的记录报告，对发生的每一起安全事件调查和解决方法都记录在案；

⑹负责定期召开等级保护管理工作会议，定期总结安全事件记录报告，并向等级保护领导小组汇报；

⑺负责建立各等级保护执行单位、关联XXX与外部安全管理主管机构之间的定期联系和沟通机制；

⑻落实纠正措施(包括审计整改意见)和预防措施。

第九条 各等级保护执行单位的主管领导的职责包括：

⑴各单位的负责任系本部门等级保护责任人，负责本部门的等级保护工作，对本部门所拥有和管理的信息资产安全负责；

⑵负责采取有效办法，落实和推动等级保护政策的实施；

⑶负责组织和建立本部门等级保护管理制度和流程，指导和要求本部门员工遵守等级保护政策；

⑷对违反安全政策的行为进行内部处罚；

⑸落实针对本部门的纠正措施(包括审计整改意见)和预防措施。

第十条 等级保护工作联络员的职责包括：

⑴负责本部门日常的具体等级保护工作，并参加等级保护工作小组所要求的各项活动；

⑵负责向等级保护工作小组负责人报告等级保护事件和违反等级保护政策的行为，协助对违反安全政策的行为进行调查；

⑶协助等级保护工作小组负责人和本部门等级保护主管领导落实针对本部门的纠正措施(包括审计整改意见)和预防措施。

第十一条 安全管理员职责：信息安全管理员是负责医院信息安全实施具体的安全措施、落实安全管理制度，维护信息系统安全的专职人员，不能兼任其他技术管理角色，如安全审计员、网络或系统管理员等。其他管理员角色可根据部门工作特点进行兼职。

第十二条 安全管理员的安全职责包括：

⑴参与XXX安全管理体系的规划、制定；

⑵学习和执行XXX制定的各项信息安全管理策略、制度、规范和指南；

⑶负责信息安全设备和产品的日常维护（包括防火墙、NIDS、防病毒软件、内网管理、上网行为管理等）；

⑷负责处理有关信息安全事件，根据信息安全事件的处理情况提交事件处理报告；

⑸组织和参加XXX的信息安全巡检和审核工作；并在其他管理员的协助下建立完整的安全巡检和审核报告，及时向管理小组提交报告；

⑹根据网络系统安全需求，向信息安全管理小组汇报信息安全现状，提出安全整改意见；

⑺指导和监督其他管理员和普通用户与安全相关的工作；

⑻监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见，进行必要的安全管理体系修订；

⑼ 配合进行信息安全培训；

⑽ 与信息安全有关的其它事务。

第十三条 安全审计员安全职责:安全审计员是指定的进行日常安全管理审计工作的相关岗位。其安全职责包括：

⑴学习和执行XXX制定的各项信息安全管理策略、制度、规范和指南；

⑵定期审计各操作系统、数据库系统、网络设备（包括负载均衡设备）、安全设备和产品（防火墙、NIDS、防病毒软件、行为审计系统等）日志，对日志进行详细分析并提交

分析报告；

⑶定期审计各操作系统、数据库系统、网络设备、安全设备安全策略的配置和管理，提交分析报告；

⑷定期审计系统管理员、网络管理员等的日常操作记录，审计数据备份或恢复记录，审计机房进出记录和机房值班记录等；

⑸ 协同安全管理员和安全员制定安全管理策略；

⑹ 参加和配合XXX的信息安全巡检和审核工作；

⑺ 组织安全事件的事后追查工作；

⑻ 与信息安全有关的其它事务。

第十四条 数据库管理员的安全职责: 数据库管理员是指XXX专职的数据库管理维护岗，其安全职责包括：

⑴学习和执行XXX制定的各项信息安全管理策略、制度、规范和指南；

⑵负责数据库系统的日常运行、管理和维护，保持数据库系统处于良好的运行状态；

⑶负责对所管理的数据库系统进行日常维护和检查，并将安全设置的情况报安全管理员备案；

⑷参加和配合XXX的信息安全巡检和审核工作，并记录相关结果；

⑸在每个业务系统工程验收后，对所涉及的数据库系统做相应的安全设置，删除测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要符合保密性要求；

⑹ 制定完备的数据备份和恢复计划和演练；

⑺监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见；

⑻与数据库维护安全相关的其他事项。

第十五条 网络管理员的安全职责：网络管理员是指XXX专职的网络管理维护岗，其安全职责包括：

⑴学习和执行XXX制定的各项信息安全管理策略、制度、规范和指南；

⑵负责网络设备的日常运行、管理和维护，保持系统处于良好的运行状态；

⑶负责对所管理的网络设备进行日常维护和检查，并将安全设置的情况报安全管理员备案；

⑷参加和配合XXX的信息安全巡检和审核工作，并记录相关结果；

⑸在每个网络系统工程验收后，对工程所涉及的网络设备、网络服务作相应的安全设置，删除设备的测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要

符合保密性要求；

⑹编制网络设备的维修、报损、报废计划，报XXX信息技术主管部门审核；

⑺监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见；

⑻与网络维护安全相关的其他事项。

第十六条 系统管理员的安全职责：系统管理员是指XXX专职的系统管理维护岗，其安全职责包括：

⑴学习和执行XXX制定的各项信息安全管理策略、制度、规范和指南；

⑵负责主机系统的日常运行、管理和维护，保持系统处于良好的运行状态；

⑶负责对所管理的主机系统进行日常维护和检查，并将相关安全设置的情况报安全管理员备案；

⑷参加和配合XXX的信息安全巡检和审核工作，并记录相关结果；

⑸在每个信息系统工程验收后，对工程所涉及的主机系统作相应的安全设置，删除系统的测试账号，对需要保留的账号口令重新进行设置，并且在口令的设置上要符合保密性

要求；

⑹编制计算机设备的维修、报损、报废计划，报XXX信息技术主管部门审核；

⑺监控信息系统的安全需求变化，及时获取来自其他管理员和普通用户的安全意见；

⑻与系统维护相关的其他事项。

第十七条 稽查部的职责包括：

⑴负责对XXX各部门和下属单位的等级保护或某个主题进行定期审计或信息安全专项审计；

⑵主要以等级保护管理政策及各种标准规范作为审核依据；在具体的审核过程中，必要时可获得等级保护领导小组的协助与支持；

⑶ 负责汇报审计结果，并督促审计整改工作的进行。

## 第六章持续改进

第十七条 为了保证本文件的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第七章附则

第十八条 本文件由技术中心负责制定、解释和修改。

第十九条 本文件自发布之日起执行。

### 附录一XXX院会议纪要

信息安全等级保护工作组织架构会议纪要

■会议时间：

■会议地点：

■参会人员：

■缺席人员：

会议内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 信息安全岗位表 | | | | |
| 岗位名称 | 负责人 | 联系电话 | 所属部门 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附录二XXX信息安全岗位表

# 四、安全检查管理规定

## 第一章总则

第一条 为规范XXX信息安全检查工作流程，明确职责，有效地进行安全检查，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX信息安全检查准备、实施、报告和整改过程。

## 第三章术语定义

第三条 安全检查：指XXX内部或外部机构对信息安全整体执行情况进行的评价活动。安全检查的依据是监管机构、XXX现行的管理制度、信息系统安全体系规范和技术标准、有关法律、法规和标准要求等，安全检查包括安全例行检查、安全专项检查等。

第四条 安全例行检查：指按照已制定的检查周期所作的检查。

第五条 安全专项抽查：指根据监管机构、XXX或相关部门要求的安全运行状况所作的不定期的抽查。

## 第四章组织职责

第六条 安全管理员负责牵头协调组织各系统信息安全检查的管理工作。

第七条 相关人员应配合安全检查，如实提供所需要的检查信息，对安全检查所发现的问题制定整改措施、整改计划并实施整改。

## 第五章通用要求

第八条 安全检查应当遵循全面、审慎、独立的原则。

第九条 应当定期对信息系统进行安全检查，检查内容应包括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。

第十条 可根据实际需要组织专项检查，对于信息系统发生的重大事故和问题，要进行专项检查，对重大事件实施全面的监控和评价。

第十一条 对于新系统，包括设备、主机、应用系统上线或安装前必须经过安全检查，检查方式应包括系统安全配置，漏洞评估，恶意代码检测，根据检查结果进行整改后方可上线。

第十二条 必须对检查工具、检查过程信息和检查结果信息的使用和访问采取控制措施加以保护，以防止任何可能的风险。

第十三条 定期（至少每年一次）对信息系统开展安全检查工作。

## 第六章安全检查准备

第十四条 安全管理员应组织相关部门或人员按照检查周期进行安全例行检查，根据需要组织安全专项检查。

第十五条 安全检查应按照所规定的检查要点、检查方式、使用规定的检查工具进行检查。

第十六条 应选择对XXX信息系统运行影响最小的方式和时间进行检查。

第十七条 对生产环境实施安全检查应按照有关信息系统变更管理规定的变更流程执行。

第十八条 实施对生产环境可能造成影响的安全检查后，应协调相关部门或人员对检查结果进行验证。

第十九条 安全检查可采用抽查的方式进行，抽查的采样量应能确保安全检查结果的准确性、代表性并符合系统实际生产情况。

第二十条 检查过程中应做好检查结果的记录工作。

## 第七章 安全检查报告

第二十一条 检查完成后由安全管理员负责组织编写检查报告并提出整改建议（附录一安全检查情况汇总表），提供给相关部门。

## 第八章安全检查整改

第二十二条 相关部门应按照检查报告中整改的时间要求，针对检查报告中所提出的问题制定整改实施计划并组织整改。

第二十三条 安全管理员应对整改措施的落实情况进行跟踪，验证整改措施的实施结果是否有效，必要时可进行复查确认。

第二十四条 安全管理员根据检查结果和整改情况进行汇总，形成安全状况通报并提供给相关部门。

## 第九章检查工具的使用

第二十五条 在安全检查过程中如果需要使用安全工具，只能使用经过审核过的安全检查工具。

第二十六条 安全检查工具只能在检查设备或者被检查部门的设备上运行，并由检查人员负责操作。

第二十七条 在生产系统中使用检查工具前，安全管理员要组织进行测试工作，对其可能产生的影响进行评估和论证，必要时安排双人进行操作。

## 第十章持续改进

第二十八条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十一章附则

第二十九条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第三十条 本文件自发布之日起执行。

### 附录一安全检查汇总表

安全检查汇总表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 不符合项 | 具体内容 | 原因说明 | 改善建议 | 负责人/部门 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |

共有主要不符合项：

注：1.检查人员为安全管理员，责任人为相应业务系统负责人。

2.此表根据现场检查科目及情况可做适当修改。

3.此表每 90天一张，为现场检查依据，除签名处外其他均由安全管理员填写。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 日期 | 检查业务部门 | 检查人员 | 负责人/部门 | 不符合项目知晓情况 |
| 1 |  |  |  |  |  |
| 2 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 5 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |
| 8 |  |  |  |  |  |
| 9 |  |  |  |  |  |
| 10 |  |  |  |  |  |

### 附录二安全检查记录表

安全检查记录表

|  |  |
| --- | --- |
| 供电故障次数、原因及恢复措施 | 无 |
| 电源定期维护情况 | 无 |
| 网络故障次数、原因及恢复措施 | 无 |
| 网络调整、切换情况及原因 | 无 |
| 设备定期维护情况 | 无 |
| 主机系统故障次数、原因及恢复措施 | 无 |
| 主机系统定期维护情况 |  |
| 系统临时重启情况及原因 |  |
| 应用系统故障次数、原因及恢复措施 |  |
| 应用系统维护情况 |  |
| 数据处理中心遭火灾、水灾、雷击、人为破坏情况及范围  况及范围 |  |
| 信息系统计算机病毒感染次数、范围、原因及恢复措施 |  |
| 网络遭遇入侵或攻击频率及范围 |  |
| 其他信息安全主管部门的安全要求、检查和调研情况 |  |

1、信息系统安全事件情况

下表各项内容如实填写，无情况的必须明确注明“无”

2、信息系统安全管理情况

2.1 组织机构

说明信息系统安全组织机构变化情况。

2.2 标准制度规范

说明信息系统安全制度、标准、规范变化情况。

2.3 安全培训、教育

说明员工安全培训及交流情况。

3、信息系统安全系统建设

说明新增、购买、升级专门的信息系统安全软硬件设备或其他应

用系统中安全部件的情况。

4、信息系统安全控制

说明信息系统新建、改造、升级、投产的安全控制和审查情况。

5、信息系统安全运行

5.1 信息系统巡检

说明信息系统定期巡检情况。参考《巡检记录表\_11月》

5.2 应急演练

说明信息系统应急计划、方案演练情况。参考《迁移实施计划》

6、安全隐患

说明发现的安全隐患和解决方案、计划。

7、建议与意见

说明对信息系统安全建设建议与意见。

8、总结

对本行当前阶段信息系统安全的结论性说明。

说明：

1、本报告分书面和电子两种形式，上报用电子邮件，签章的书面

材料 XXX 留存，以被核实和调阅。

2、供电系统主要指中心机房，灾备机房。

# 五、人力资源信息安全管理规定

## 第一章总则

第一条 本规范目标在于建立XXX员工人力资源信息安全管理制度，用于规范对员工招聘、录用、离职等过程的信息安全控制。

## 第二章适用范围

第二条 本文件适用于XXX内部所有员工。

## 第三章术语定义

第三条 本XXX内部所有员工是指XXX正式员工，包括试用期员工和借调人员等。

## 第四章组织职责

第四条 XXX技术中心负责员工入职、在职、离职等过程涉及的信息安全管理和控制。

## 第五章入职信息安全管理

第五条 技术中心协助人力资源部确保人员在任用前，在适当的岗位描述、任用条款和条件中明确说明其应履行的信息安全职责，确保其人员理解其信息安全职责，确保人员承担的角色符合XXX的信息安全要求。

第六条 技术中心要对任用的员工候选人员进行充分的信息安全审查。

第七条 员工筛选

⑴技术中心协助人力资源部负责组织对XXX各个职位的应聘人员进行筛选、对应聘人员涉及信息安全方面的资料核实和背景调查。

⑵对员工的背景调查应在申请职位时进行。信息安全方面的调查内容包括以下：

①申请人的信息安全风险认识考察；

②监管部门相关的信息安全要求；

③其它需要调查的内容。

第八条 出于背景调查目的收集、处理被调查人员信息时，应在不违反相关的法律法规的前提下进行。

第九条 安全职责

⑴对于员工，必须对其信息安全角色和职责进行描述和说明。

⑵安全职责应包括但不限于以下要求：

①遵守XXX信息安全方面的各项规章制度；

②按照XXX的要求实施各项安全控制措施；

③按照要求组织、参与或配合XXX的各项信息安全检查活动；

④保护XXX的信息资产免受非授权访问、泄露、修改和破坏；

⑤积极参加各项信息安全培训；

⑥报告安全事件、潜在安全事件、以及其他可能引发安全风险的事件。

第十条 任用条款和条件

⑴人力资源部门组织员工签署保密协议。

⑵保密条款或保密协议具有法律效力，保密协议或包含保密条款的合同在签订前，应经过XXX相关部门的合规性审查，以避免法律法规风险。

## 第六章在职信息安全管理

第十一条 员工使用XXX网络访问权限或应用系统帐号时，需由员工所在部门提出申请,技术中心根据工作需要，按最小权限原则开通相关的工作帐号。

第十二条 员工工作岗位发生变化时，人力资源部门应及时通知技术中心，对其访问权限和系统帐号进行相应的调整。

第十三条 技术中心应协助人力资源部对XXX所有员工进行与工作职能相关的信息安全意识培训和教育。

第十四条 纪律处理过程

⑴对于信息安全违规的人员，在正式纪律处理之前,技术中心应对信息安全违规进行评估和确认,提交人力资源部门相关信息安全违规评估报告；

⑵对内部员工的具体纪律处理执行参照人力资源部门相关规定。

## 第七章调动信息安全管理

第十五条 人员调动按XXX相关规定完成相应流程办理后，由人力资源部通知，技术中心负责完成调动员工相关权限和应用系统帐号的变更工作。

第十六条 技术中心应协助人力资源部门监督转岗人员完成个人办公电脑中业务资料、应用系统帐号密码等工作的交接。

第十七条 转岗人员在完成工作交接后，对于新工作中不需要使用到原工作中的业务资料，其个人办公电脑硬盘由技术中心负责进行数据清除，清除方式包括格式化或使用专用工具进行安全擦除。

第十八条 技术中心应协助稽查部完成对转岗人员离岗前的信息安全方面的稽核工作。

## 第八章离职信息安全管理

第十九条 任用终止职责

⑴技术中心应协助人力资源部清晰的定义员工任用终止的职责，包括收回帐号、密码更改等；

⑵安全管理员应及时关闭离职人员的访问账号及权限；

⑶安全管理员应对离职人员办理离职手续期间访问日志进行审计。

第二十条 信息资产归还

⑴所有的员工在终止任用合同或协议时，应归还其使用的所有XXX信息资产。需要交接的信息资产包括计算机设备、工作证、纸质文件资料和存储于电子介质中的文档、数

据等。离职人员办公电脑中的数据由其所在部门决定如何处置，归还后的办公电脑操作系统盘由技术中心进行格式化；

⑵当员工在XXX工作期间，利用XXX信息资产产生信息及其知识产权，除另有约定外，属于XXX所有。

第二十一条 撤销访问权限

⑴所有员工对信息和信息处理设施的访问权限应在任用终止时注销或删除；

⑵技术中心负责注销或删除访问权的内容包括物理访问授权、逻辑访问授权。必要时，在对信息和信息处理设施的访问权限终止前需要进行风险评估。

## 第九章持续改进

第二十二条 为了保证本文件的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章 附则

第二十三条 本文件由XXX技术中心负责解释。

第二十四条 本文件自印发之日起施行。

|  |  |  |  |
| --- | --- | --- | --- |
| 人员信息安全审查记录 | | | |
| 审查名称 |  | 时间 | 2 |
| 发起部门 |  | | |
| 考核记录 | | | |
| 姓名 | 所属部门 | 时间 | 审查结果 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 备注 |  | | |
| 审查人签字 |  | 签字日期 |  |
| 审核意见 |  | | |
| 部门领导  审核签字 |  | 签字日期 |  |

### 附录一XXX人员安全审查记录

**广州XXX医药有限医院人员信息安全审查记录**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 被考核人员 |  | 负责人 |  | | 考核时间 | |  |
| 安全规范执行情况 |  | | | | | | |
| 存在的问题 |  | | | | | | |
| 考核意见 |  | | | | | | |
| 考核部门 | 技术中心 | | | 考核负责人 | |  | |

### 附录二XXX人员录用安全考核记录表

**广州XXX医药有限医院人员录用信息安全考核记录表**

### 附录三XXX关键岗位安全协议

**员工保密协议**

　　甲方(企业)：\_ \_\_\_\_\_

　　乙方(员工)：\_

　　鉴于乙方在甲方任职，并将获得甲方支付的相应报酬，双方当事人就乙方在任职期间及离职以后保守甲方商业秘密的有关事项，制定下列条款共同遵守：

1. 商业秘密的内容

本协议提及的商业秘密包括技术秘密和经营秘密，其中技术秘密包括但不限于工作进度、技术方案、数据库、研究开发记录、技术报告、技术文档、相关的函电等；经营秘密包括但不限于客户资料、行销计划、采购资料、定价政策、财务资料、进货渠道、法律事务信息、人力资源信息等等。

1. 保密规章和制度

乙方在任职期间必须遵守甲方的保密规章、制度，履行与其工作岗位相应的保密职责。遇到甲方保密规章、制度中未规定或者规定不明确的方面时，乙方应本着谨慎、负责的态度，采取必要、合理的措施，保守其于任职期间知悉或者持有的任何属于甲方或者虽属于第三方但甲方承诺有保密义务的商业秘密。  
  
第三条保密责任  
  
除履行职务需要之外，未经甲方事先书面同意，乙方不得泄漏、传播、公布、发表、传授、转让、交换或者以其他任何方式使任何第三方（包括无权知悉该项秘密的甲方职员）知悉属于甲方或者属于第三方但甲方承诺有保密义务的商业秘密，也不得在履行职务之外使用这些秘密信息。

第四条保密期限  
  
甲乙双方确认，乙方的保密义务自甲方对本协议第一条所述的商业秘密采取适当的保密措施并告知乙方时开始，到该商业秘密由甲方公开时止。  
  
无论乙方因何种原因离职，乙方离职之后（自离职之日起）仍应当保守在甲方任职期间接触、知悉的属于甲方或者虽属于第三方但甲方承诺有保密义务的商业秘密，承担同在甲方任职期间一样的保密义务。乙方自离职之日起半年内不得去竞争对手医院（网上药店和保健品网上销售医院）工作。

第五条 从事第二职业的限制  
  
乙方承诺在甲方任职期间，不从事第二职业。特别是未经甲方书面同意，不得在与甲方生产、经营同类产品或提供同类服务的其他企业内任职，包括但不限于合伙人、董事、监事、股东、经理、职员、代理人、顾问等；不得间接为上述企业提供服务。  
  
第六条秘密信息的载体  
  
乙方因职务上的需要所持有或保管的一切记录有甲方秘密信息的电脑、文件、资料、图表、笔记、报告、信件、传真以及其他任何形式的载体均归甲方所有，无论这些秘密信息有无商业上的价值。  
  
乙方应当于离职时，或者于甲方提出要求时，返还属于甲方的全部财物和载有甲方秘密信息的一切载体，不得将这些载体及其复制件擅自保留或交给其他任何单位或个人。  
  
第七条任职期间  
  
本协议中所称的任职期间，是指乙方从甲方领取工资到甲方终止向乙方发放工资或乙方不再从甲方领取工资为止的期间。  
  
本协议中所称的离职，是指任何乙方明确表示解除聘用关系并将此种意愿付诸事实的行为，包括辞职、辞退等正常离职和非正常离职。  
  
第八条侵权责任  
  
甲、乙双方约定：  
  
（1）如果乙方不履行本协议所规定的保密义务，应当承担违约责任，任职期间接受甲方的罚款、降薪或辞退等处罚；如已离职，一次性向甲方支付违约金1万元人民币元；  
  
（2）如果因为乙方前款所称的违约行为造成甲方的损失，乙方应当承担违约责任，并承担赔偿甲方损失的责任。  
  
（3）前款所述损失赔偿按照如下方式计算：  
  
①损失赔偿额为甲方因乙方的违约行为所受到的实际经济损失；  
  
②如果甲方的损失依照①款所述的计算方法难以计算的，损失赔偿额为乙方因违约行为所获得的全部利润；或者以不低于甲方商业秘密许可使用费的合理数额作为损失赔偿额；  
  
③甲方因调查乙方的违约行为而支付的合理费用，应当包含在损失赔偿额之内；  
  
（4）因乙方的违约行为侵犯了甲方的商业秘密权利的，甲方可以选择根据本协议要求乙方承担违约责任，或者根据国家有关法律、法规通过司法的方式要求乙方承担侵权法律责任。  
  
第九条争议解决  
  
因本协议而引起的任何纠纷由双方协商解决；如果协商不成，任何一方均可以在广州市黄埔区人民法院提起诉讼。  
  
上述约定不影响甲方请求知识产权管理部门对侵权行为进行行政处理。  
  
第十条其它事项  
  
本协议如与双方以前的任何口头或书面协议有抵触，以本协议的规定为准。  
  
本协议的修改必须采用书面形式。  
  
本协议正本一式二份，甲乙双方各执一份。  
  
第十一条生效  
  
本协议自双方签字盖章之日起生效。

甲方：乙方签字：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
代表：身份证号：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
  
签字日期：\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日签字日期：\_\_\_\_\_\_年\_\_\_\_月\_\_\_\_日

# 六、信息安全培训和考核管理规定

## 第一章总则

第一条 为了提高XXX员工信息安全意识和相关人员的安全技能，向全体员工宣讲信息安全管理的各项法规制度，将可能的风险降到最低，明确信息安全培训与考核管理过程与职责，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX信息安全培训与考核管理过程。

## 第三章术语定义

略............

## 第四章 组织职责

第三条 信息安全培训与考核工作由技术中心负责组织、筹备，须遵循相关的人力资源部门培训制度。

第四条 安全管理员负责具体落实具体的培训与考核内容、培训与考核形式、登记汇总以及相关事宜。

第五条 人力资源部门负责协调组织相关培训与考核联系工作、并将培训与考核相关数据纳入相关人事考核指标。

## 第五章安全培训管理程序

第六条 安全培训主要包括安全意识培训、安全技能培训以及专业技术培训。

第七条 安全意识培训会因不同的对象有所调整，建议全员参与，在某些情况下可以要求有关的第三方组织参加。

培训的内容可以包括：

⑴对在职职工进行必要的信息安全教育培训，让职工了解和掌握信息安全法律法规，加强全体职工的安全生产意识。

⑵为提高XXX员工的综合素质，XXX采用各种方式对员工进行内部在职培训。如举办安全知识讲座、安全知识竞赛、简报、发放宣传品等形式。

⑶在XXX内组织举办定期或不定期的业务学习班。由专业人员对员工进行业务培训。

⑷根据XXX业务发展需要，对相关业务骨干人员组织送培，到相关业务单位进修及相关学院委托培养。

⑸为强化在职培训效果，XXX定期组织多种形式的培训考核。

第八条 安全技能培训主要是针对信息处理设备使用者或管理人员进行的，如系统安全配置，开发安全配置等 IT安全技术相关内容。

第九条 专业技术培训是专门针对信息安全工作需要设立的，如 ISO 27001、CISSP 等专业安全培训。

第十条 培训类型可采用内部培训或外部培训（聘请外部专家），由XXX聘请专家顾问以及其他专业人员对员工进行培训。

第十一条 信息安全培训应由安全管理员进行汇总登记

（附件一，信息安全培训汇总登记表）。

第十二条 安全意识培训

⑴安全意识培训工作应当由技术中心负责组织和准备，在人力资源部和其他部门的配合下开展。

⑵全体员工应该参加关于信息安全方面的培训。

⑶新进员工应当在入职后 3 个月内参加信息安全培训。

⑷关键/敏感岗位的人员的变动应当开展相关的岗位培训。

⑸对信息安全政策、制度、标准的重大调整、更新必须组织相关培训，保证所有员工及时了解、掌握变更内容。

⑹用户在使用任何信息技术设施前（包括软件和硬件），必须接受完整的培训，特别是应当包括关于XXX各项使用规定。

第十三条 安全技能培训

⑴技术中心负责组织培训工作，安全技能培训的教材、课程应当由安全管理员负责，保证所有需要参加培训的人员都能及时的参加必要的安全技能培训。

⑵当系统的新建、升级对用户使用产生影响时，必须事先开展必要的针对用户的培训。

第十四条 专业安全技术培训

⑴专业技术培训主要是针对技术人员开展的。可以采用内部培训的方式由经验丰富的高级技术人员来传授知识，也可以请供应商或者其他第三方提供专业的培训，但外包培训应当尽可能避免接触XXX的敏感信息。

⑵技术中心应派遣技术人员参加外部举办的安全相关训练、研讨会或产品展示会，及时掌握最新的安全技术。

⑶技术人员可以提出申请(附件二，XXX专业技术培训申请审批表)，由相关部门审批后参加专业安全技术培训。

## 第六章安全考核管理程序

第十五条 信息安全考核至少一年进行一次全面的信息安全考核，由技术中心负责组织相关部门或人员成立考核小组进行信息安全考核工作。

第十六条 普通员工可以通过安全问卷的方式进行考核，考核内容按照(附件三，员工信息安全考核表)中相关内容进行考核。

第十七条 由安全管理员制定信息安全关键岗位考核内容，考核内容应包括安全管理制度落实情况、安全培训情况以及安全技能相关内容，可参照（附件四，信息安全关键岗位考核内容表），并报技术中心领导审批。

第十八条 信息安全关键岗位考核内容应根据不同岗位进行区分，具体考核指标关系见（附件五，信息安全关键岗位考核指标对应表）。

第十九条 信息安全考核结果应及时汇总、登记（附件六、信息安全考核汇总登记表）。

## 第七章持续改进

第二十条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第八章附则

第二十一条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第二十二条 本文件自发布之日起执行。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 时间 | 地点 | 培训内容 | 培训人员/部门 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
| 5 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附件一信息安全培训汇表

（2018年）信息安全培训汇总表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 申请部门 |  | 参加对象  及人数 | |  | | | |
| 培训内容 |  | 培训类型 | | 内    训√  外    训□  公开课□ | | 培训费 |  |
| 培训时间 |  | 培训地点 | |  | | 学时 |  |
| 培训师资  及组织者  情况 |  | | | | | | |
| 培训目的 | 申请部门负责人签字： 2018 年 月 日 | | | | | | |
| 财务部门  意见 | 同 意□  不同意□  签字： 2018 年 月 日 | | 人事部门  意见 | | 同 意□  不同意□  签字： 年 月 日 | | |
| 备注 |  | | | | | | |

### 附件二专业安全技术培训申请审批表

XXX专业安全技术培训申请审批表

（规范性附录）

安全意识培训

编号：

|  |  |  |  |
| --- | --- | --- | --- |
| 姓名： | 部门： | 日期：年 月 日 | 被考核人签名： |
| 安全需求 | | 状况（是/否/n/a） | 说明 |
| 开机口令 | | | |
| 口令长度是否大于 8 位？ | |  |  |
| 口令中是否包含数字？ | |  |  |
| 屏保 | |  |  |
| 是否在 15 分钟的非活动状态内自动激活  带密码保护的屏保？ | |  |  |
| 密码长度是否大于 8位？ | |  |  |
| 密码中是否包含数字？ | |  |  |
| 工作结束时，是否关闭或锁定台式计算  机？ | |  |  |
| 工作结束时，是否妥善保管便携电脑，如锁入文件柜？ | |  |  |
| 软件 | |  |  |
| 办公用机是否擅自改变预安装软件？ | | 否 |  |

### 附件三员工信息安全考核表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 关键考核指标 | 指标说明 | 考核频度 | 数据来源 | 备注 |
| 安全制度遵守情况 | | | | |
| 信息安全政策规范遵  守执行情况 | 对于信息安全策略与标  准中所制定的各项控制  措施的遵守执行情况 | 年末考核 | 日常安全事务记  录、访谈结果或  内部审计报告 | 对信息安全政  策规范遵守执  行情况也可以  通过访谈或者  内部审计报告  获得 |
| 参加安全培训情况 | | | | |
| 参加安全相关培训时  间 | 信息安全管理/技术关  键岗位人员参加培训的  实际小时数与目标小时  数的比率的加权平均 | 年末考核 | 安全培训登记表 |  |
| 参加安全相关培训成  绩 | 当员工所参加的安全相  关培训时间超过年工作  时间的 5％时，将员工  参加此类培训所取得的  成绩取加权平均 | 年末考核 | 安全培训登记表 | 本考核指标仅  当员工所参加  的安全相关培  训时间超过当  年工作时间的  5％时有效 |
| 安全技术指标 | | | | |
| 网络连通率 | 当年网络连通时间与全  年时间的比率 | 年末考核 | 网络日志、维护  报告 |  |

信息安全关键岗位考核内容表

### 附件四关键岗位考核内容表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 关键考核指标 | 指标说明 | 考核频度 | 数据来源 | 备注 |
| 非正常运行时间 | 当年系统宕机、中断服  务的累计时间 | 年末考核 | 系统日志、维护  报告 | 正常的系统维  护停机时间不  包含在本指标  中。可根据系  统自动产生的  日志文件和维  护记录统计非  正常宕机、中  断服务的总时  间。 |
| 安全事件数量 | 当年安全事件发生数量 | 年末考核 | 安全事件汇总记  录表 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 考核指标 | 信息安全关键岗位 | | | | | | | |
| 安全管理员 | | | 网络管理员 | 设备管  理员 | 系统管理员  数据库 | 系统管  理员 | 项目开发管理员 |
| 安全制度遵守情况 | | | | | | | | |
| 信息安全政策规范遵守执行情况 |  | | |  |  |  |  |  |
| 参加安全培训情况 | | | | | | | | |
| 参加安全相关培训时间 | |  |  | |  |  |  |  |
| 参加安全相关培训成绩 | |  |  | |  |  |  |  |
| 安全技术指标 | | | | | | | | |
| 网络连通率 |  | | |  |  |  |  |  |
| 系统非正常运行时间 |  | | |  |  |  |  |  |
| 安全事件数量 |  | | |  |  |  |  |  |

### 附件五关键岗位考核指标对应表

**信息安全关键岗位考核指标对应表**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 姓名 | 部门 | 考核内容 | 得分 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 4 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附件六信息安全考核汇总表

信息安全考核汇总表

备注：1、考核内容填写普通员工考核、信息安全关键岗位考核。

### 附件七人员培训记录表

人员培训记录表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 培训组织部门 | |  | | 培训时间 | |  | |
| 培训教师 | |  | | 培训地点 | |  | |
| 培训目的 | |  | | | | | |
| 培  训  主  要  内  容 |  | | | | | | |
| 培训  人员  名单  (签名) | 姓    名 | | 部    门 | | 姓    名 | | 部    门 |
|  | |  | |  | |  |
|  | |  | |  | |  |
|  | |  | |  | |  |
|  | |  | |  | |  |
|  | |  | |  | |  |
|  | |  | |  | |  |
|  | |  | |  | |  |

### 附件八年培训调查（计划）表

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 课程名称 | 培训目标 | 培训对象 | 培训方式 | 课时 | 讲师 | 培训费用 | 培训责任人 | 备注 |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |

# 七、信息系统等级保护建设管理规定

## 第一章总则

第一条 为了规范信息安全等级保护管理，提高信息安全保障能力和水平，维护信息系统安全运行，保障和促进信息化建设，根据公通字 2007[043]《信息安全等级保护管理办法》，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX信息系统等级保护建设过程，管理对象为等级保护建设过程中所有应定级和已定级系统

## 第三章组织职责

第三条 信息安全等级保护工作领导小组（以下简称等级保护领导小组）的职责见《XXX等级保护管理组织架构规定》的要求。

第四条 信息安全等级保护工作工作小组（以下简称等级保护工作小组）的职责见《XXX等级保护管理组织架构规定》的要求。

第五条 安全管理员的职责见《XXX等级保护管理组织架构规定》的要求。

第六条 我院相关部门或人员协助配合安全管理员进行等级保护建设工作。

## 第四章系统定级

第七条 信息系统定级坚持自主定级、自主保护的原则。信息系统的安全保护等级应当根据信息系统在国家安全、经济建设、社会生活中的重要程度，信息系统遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等因素确定。

第八条 信息系统的安全保护等级分为以下五级：

第一级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益造成损害，但不损害国家安全、社会秩序和公共利益。

第二级，信息系统受到破坏后，会对公民、法人和其他组织的合法权益产生严重损害，或者对社会秩序和公共利益造成损害，但不损害国家安全。

第三级，信息系统受到破坏后，会对社会秩序和公共利益造成严重损害，或者对国家安全造成损害。

第四级，信息系统受到破坏后，会对社会秩序和公共利益造成特别严重损害，或者对国家安全造成严重损害。

第五级，信息系统受到破坏后，会对国家安全造成特别严重损害。

第九条 由安全管理员根据《GB/T 22240 信息安全等级保护定级指南》中等级保护定级因素、以及监管部门的要求对系统进行定级。

第十条 安全管理员制订信息系统定级报告，并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。

第十一条 审定通过的定级报告报送相关等级保护主管部门进行审批。

## 第五章安全检查报告

第十二条 安全方案设计阶段的目标是根据信息系统的划分情况、信息系统的定级情况、信息系统承载业务情况，通过分析明确信息系统安全需求，设计合理的、满足等级保护要求的总体安全方案，并制定出安全实施计划，以指导后续的信息系统安全建设工程实施。对于已运营（运行）的信息系统，需求分析应当首先分析判断信息系统的安全保护现状与等级保护要求之间的差距。

第十三条 安全管理员协调相关部门或人员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。

第十四条 安全管理员协调相关部门或人员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。

第十五条 等级保护领导小组负责组织相关部门和有关安全技术专家对系统安全设计方案进行评审和论证。

第十六条 根据等级测评、安全评估的结果由安全管理员协调相关人员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。

## 第六章系统建设

第十七条 产品采购和使用应按照国家安全相关部门要求和XXX相关管理制度进行产品采购。

第十八条 系统建设完成后可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；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，对不符合等级保护要求的及时进行整改，并形成测试验收报告。

第十九条 安全管理员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。

第七章系统备案

第二十条 已运营（运行）的第二级以上信息系统，应当在安全保护等级确定后 30 日内，由安全管理员到所在地区的市级以上公安机关办理备案手续。

第二十一条 新建第二级以上信息系统，应当在投入运行后 30 日内，由安全管理员到所在地区的市级以上公安机关办理备案手续。

第二十二条 办理信息系统安全保护等级备案手续时，应当填写《信息系统安全等级保护备案表》，第三级以上信息系统应当同时提供以下材料：

⑴系统拓扑结构及说明

⑵系统安全组织机构和管理制度；

⑶系统安全保护设施设计实施方案或者改建实施方案；

⑷系统使用的信息安全产品清单及其认证、销售许可证明；

⑸测评后符合系统安全保护等级的技术检测评估报告；

⑹信息系统安全保护等级专家评审意见；

⑺主管部门审核批准信息系统安全保护等级的意见。安全检查工具只能在检查设备或者被检查部门的设备上运行，并由检查人员负责操作。

## 第七章系统测评

第二十三条 测评机构应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，第三级以上信息系统应当选择符合下列条件的等级保护测评机构进行测评：

⑴在中华人民共和国境内注册成立（港澳台地区除外）；

⑵由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

⑵由中国公民投资、中国法人投资或者国家投资的企事业单位（港澳台地区除外）；

⑶从事相关检测评估工作两年以上，无违法记录；

⑷工作人员仅限于中国公民；

⑸法人及主要业务、技术人员无犯罪记录；

⑹使用的技术装备、设施应当符合本办法对信息安全产品的要求；

⑺具有完备的保密管理、项目管理、质量管理、人员管理和培训教育等安全管理制度；

⑻对国家安全、社会秩序、公共利益不构成威胁。

第二十四条 安全管理员负责对测评机构等级测评过程按照XXX相关规定进行管理，负责对测评人员安全保密进行要求，必要时与其签订安全保密责任书，规定应当履行的安全保密义务和承担的法律责任，并负责检查落实。

第二十五条 在系统运行过程中，应定期进行等级测评，三级及三级以上系统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。

第二十六条 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。

## 第八章系统终止

第二十七条 信息系统被转移、终止或废弃时，由安全管理员组织系统相关管理人员提出系统终止申请，由XXX等级保护领导小组进行审批，方可执行系统转移、终止或废弃。第三十条 审批通过后由安全管理对系统所属软、硬件和介质等敏感信息按照相关规定进行处理。

## 第九章持续改进

第二十八条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章附则

第二十九条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第三十条 本文件自发布之日起执行。

|  |  |
| --- | --- |
| 方案名称 |  |
| 评审人员 |  |

### 附录一系统安全设计方案评审表

系统安全设计方案评审表

|  |  |
| --- | --- |
| 方案名称 | 核心业务系统定级 |
| 评审人员 |  |
| 日期 |  |
| 方案内容(须提交方案做为附件)： | |
| 评审意见：  评审人员：  日期： | |

|  |  |
| --- | --- |
| 报告名称 | 异地备份系统验收 |
| 评审人员 |  |
| 报告内容(须提交测试报告做为附件)：  原OA服务器停机，启动英方异地备份OA服务器服务，经过业务压力测试，测  试结果正常，验收合格。 | |
| 评审意见：  评审人员：  日期： | |

日期：

年

月

日

### 附录二系统测试验收评审表

系统测试验收评审表

|  |  |
| --- | --- |
| 系统名称：新禾LIS系统 | |
| 系统申请调整状态（转移、终止或废弃）：终止 | |
| 提出部门：计算机中心 | 提出人： |
| 转移、终止或废弃原因说明：由于LIS系统现更改使用惠桥LIS系统，故终止新禾LIS系统业务。 | |
| 系统所属部门意见：同意  （ 签章 ）  2018年  1    月  15     日 | |
| 等级保护领导小组意见：  组长签字：                       年      月      日 | |

日期：

年

月

日

### 附录三系统转移、终止或废弃申请表

系统转移、终止或废弃申请表

|  |  |
| --- | --- |
| 系统名称 |  |
| 专家成员 |  |
| 定级结果 |  |
| 论证细则 | |
|  | |

专家签字：

### 附录四系统定级专家论证文档

系统定级专家论证文档

### 附录五系统维护手册（模板）

本模板用于供各等级保护系统制作维护手册时参考。

软件系统维护手册必须就应用系统的初始化，系统的启停、安全、故障处理，以及应用软

件和数据的备份和恢复等做出尽量详尽的说明。

第一章简介

本章将简要地说明软件系统维护手册(以下简称本手册)的目的、范围、名词定义和参考

文件。

第一条 手册目的本手册的目的在于说明系统维护人员在操作、监视和维护本系统时所应采用的方法和程序；并提供有关的信息，例如系统架构、系统运行环境、软件结构等。

第二条 手册范围手册除了说明系统维护人员在操作、监视和维护本系统时所应采用的方法和程序之外，也简要地介绍了本系统的系统架构、系统运行环境、应用软件结构等。对于系统的安装以及应用软件等操作使用方面的内容，请参考本系统的《安装手册》及《操作手册》。本手册的使用者为系统维护人员。

本手册各章节内容安排如下：

• 第一章 简介：简单说明本手册的目的、范围、名词定义和参考文件。

• 第二章 系统概述：简要说明本系统的系统架构、系统运行环境及应用软件结构。

• 第三章 系统准备：说明在可以启动应用系统之前, 应该执行的初始化工作和各项参数

配置。

• 第四章 系统启动、关闭：说明服务器、客户机、数据库系统及应用系统的启动与关闭

规程。

• 第五章 系统日常维护：描述系统的日常维护操作、方法。

• 第六章 安全管理：说明与系统操作维护有关之安全措施及管理方法。

• 第七章 日志管理：说明系统日志的组成与作用。

• 第八章 日常问题处理：说明系统日常出现问题的诊断方法与处理程序。

• 附录：提供应用程序目录清单、磁盘目录结构、数据库表清单、设备及用户清单、系统维护通讯录及 FAQ。

第三条 名词定义

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

这里定义为了准确地解释本手册所需要的字头词和缩写词。这些信息也可以由手册的附录提供，或引用别的文档。

第四条 参考文件

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

这一条应给出：

参考文件清单（包含提供给用户的其他交付文档的名称）

每个参考文件的标题、索引号或文件号、发布或发表日期、出版单位等

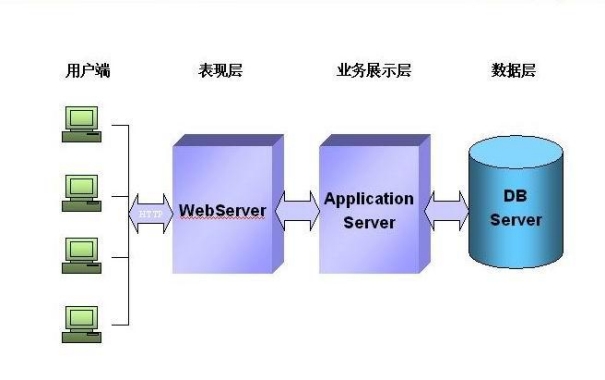
每个参考文的来源

这些信息也可以由手册的附录提供，或引用别的文档。

第二章

系统概述

第五条 系统总体架构

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

说明本系统的总体架构。

如：系统采用 B/S 架构下一系列的参数化开发组件和平台以缩短开发周期、应对需求变动和快速实施部署，保证系统充分的适应性、扩展性和灵活性。

第六条 系统运行环境

(一) 系统网络结构

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明本系统的网络组成和结构，可直接使用网络拓扑图进行表示。

(二) 系统软、硬件配置

［请在此输入正文，写完后删除下面方框和里面的参考内容。］列出本系统所涉及的硬件及相关配置，必要时可提供简要说明。系统硬件包括：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 硬件描述 | 配置/定义 | 数量 | 说明 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
| 5 |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 软件类别 | 软件名称 | 版本号 | 来源 | 说明 |
| 1 |  |  |  |  |  |
| 3 |  |  |  |  |  |
| 4 |  |  |  |  |  |
| 6 |  |  |  |  |  |
| 7 |  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| XXX系统需求框架 | | |
| 序号 | 模块名称 | 备注 |
| 1 |  |  |
| 1.1 |  |  |
| 1.1.1 |  |  |
| 1.1.2 |  |  |

括：

列出本系统所涉及的系统软件之名称、版本、来源，必要时可提供简要说明。系统软件包

(三) 应用软件功能结构

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

说明本系统的应用软件功能结构。

如：

|  |  |  |
| --- | --- | --- |
| 1.1.3 |  |  |
| 1.1.4 |  |  |
| 2 |  |  |
| 2.1 |  |  |
| 2.2 |  |  |
| 2.3 |  |  |
| 2.4 |  |  |
| 2.5 |  |  |
|  |  |  |

第七条 磁盘空间布局

这里给出各服务器和各客户机磁盘空间的布局情况，通常包括操作系统盘(区)、数据库系

统盘(区)、应用程序盘(区)、应用数据盘(区)、数据备份盘(区)、应用程序备份盘(区)等。

第三章系统准备

第八条 系统初始化

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

这里给出可以启动运行应用程序之前，必须执行的那些初始化工作。例如：

1、 安装操作系统，配置服务器名称和 IP 地址，配置网络环境等，详细信息参见附录

部分“设备及用户清单”。

2、 为操作人员创建帐户(包括操作系统帐户和数据库帐户)，设置用户权限等，详细信

息参见附录部分“设备及用户清单”。

3、 建立应用程序所使用的表空间，应用程序所使用的表、视图、存储过程、触发器、

建索引、主键等约束。

4、 加载应用程序所使用的基本数据。

系统管理员填写

第九条 服务器参数配置

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

这里给出可以启动服务器应用程序之前，必须执行的系统参数配置工作。例如建立和设定

应用程序所使用的运行参数(日志大小、并发进程数、权限设置等)。

第十条 客户机参数配置

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

［只针对 C/S 架构的系统，需要进行填写］

这里给出可以启动客户机应用程序之前，必须执行的系统参数配置工作。例如建立和设定应用程序所使用的运行参数(服务器地址、端口号、数据库设置等)。

第四章

第十一条

系统启动、关闭

数据库启动与关闭

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

数据库启动规程说明启动数据库的具体步骤、显示的系统消息、注意事项和异常处理方法等。数据库关闭规程说明关闭数据库的具体步骤、显示的系统消息、注意事项和异常处理方法等。

系统管理员填写

第十二条

应用系统启动与关闭

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

应用系统启动规程说明启动应用软件具体步骤、显示的系统消息、注意事项和异常处理方法等。应用系统关闭规程说明关闭应用软件具体步骤、显示的系统消息、注意事项和异常处理方法等。

系统管理员填写

第十三条

网络通信软件启动与关闭

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

网络通信软件启动规程说明启动服务器端和客户机端网络通信软件的具体步骤、显示的系统消息、注意事项和异常处理方法等。网络通信软件关闭规程说明关闭服务器端和客户机端网络通信软件的具体步骤、显示的系统消息、注意事项和异常处理方法等。

第十四条服务器开机与关机

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

服务器开机规程通常规定周边设备加电、主机加电、操作系统引导及操作系统登录等过程的具体步骤、注意事项和异常处理方法等。服务器关机规程通常规定操作系统关闭、关掉主机电源、关掉周边设备电源等过程的具体步骤、注意事项和异常处理方法等。系统管理员填写

第十五条

客户机开机与关机

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

客户机开机规程通常规定周边设备加电、主机加电、操作系统引导及操作系统登录等过程的具体步骤、显示的系统消息、注意事项和异常处理方法等。客户机关机规程通常规定操作系统关闭、关掉主机电源、关掉周边设备电源等过程的具体步骤、显示的系统消息、注意事项和异常处理方法等。系统管理员填写

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 用户组 | From | To | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

第五章

系统日常维护

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明本系统的日常维护工作，根据需要可划分成日维护、周维护、月维护、季度维护几个大类，每个维护各有要求，如要求每日批处理、每月提取运行统计数据等。

各种维护内容可包括下面的提示：

1、 如何执行每日批处理，批处理操作方法、步骤和注意事项

2、 如何从服务器监控整个系统的运行

3、 如何管理打印队列

4、 说明如何修改一些配置文件如打印机配置、一些环境变量的改变设置

5、 如何管理中间件产品

第六章

第十六条

安全管理

网络访问控制

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明本系统的在网络访问控制的方法，如：只允许访问的 IP 地址或网段。

第十七条

用户管理

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 用户组 | 用户名 | 权限说明 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

说明本系统的用户管理策略与方法。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 用户组 | 用户名 | 加密方式 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

第十八条

加密措施

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

说明本系统在数据传输方面采用的加密措施。

第十九条

操作系统安全

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

本节包含两方面内容：

1、 本应用系统利用操作系统所提供的安全机制，已经实现了什么样的系统安全管理。

2、 告诉系统维护人员，如何利用操作系统以及应用软件所提供的安全机制，来进一步维护系统安全

第二十条

维护系

数据库安全

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

本节包含两方面内容：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 用户组 | 用户名 | 权限说明 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

1、 本应用系统利用数据库管理系统所提供的安全机制，已经实现了什么样的数据库安

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 用户组 | 用户名 | 权限说明 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用系统 | 用户名 | 权限说明 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

全管理。

2、 如何利用数据库管理系统以及应用软件所提供的安全机制，来进一步维护系统的安

第二十一条 应用系统安全

全。

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

说明本应用系统提供了什么样的安全机制，来保证应用功能的授权使用。

第二十二条 备份及恢复

(一) 备份及恢复对象

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

备份/恢复的对象包括：







系统文件(如登录文件、用户特征文件 PROFILE、系统参数文件、命令文件……)

应用软件的程序码

应用软件有关的文件(如参数文件、头文件、批式执行文件、语音提示文件……)

数据库(包括表、索引、数据字典等)

管理员填写，参考备份 shell 文件

(二) 备份模式、命令

［请在此输入正文，写完后删除下面方框和里面的参考内容。］

说明系统备份模式、备份命令和备份周期等。系统管理员填写，参考备份 shell 文件

(三) 恢复模式、命令

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明系统恢复模式和恢复命令等。系统管理员填写，参考备份 shell 文件

第二十三条 业务可持续性运行［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明系统为保证可持续性运行所制订的相关措施与管理方法。（例如冷、热备份、双机运行、容错处理、灾难恢复等）

第七章

日志管理

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明本系统日志的组成、作用与记录内容。

第八章

日常问题处理

［请在此输入正文，写完后删除下面方框和里面的参考内容。］说明系统日常问题处理的诊断方法与处理程序，可包括：

1、 硬件/软件/中间件可能的异常状况

2、 执行故障诊断的步骤，上报流程

3、 诊断信息及相对应的动作

4、 须参考之文件

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 设备描述 | 机器名 | IP 地址 | 备注 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 目录路径 | 机器名 | IP 地址 | 备注 |
| 1 | /home/vbs4 |  |  |  |
| 2 |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 所属部门或系统 | 姓名 | 电话 | 管理属性 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |

# 八、工作环境管理规定

## 第一章总侧

第一条 为加强XXX办公区域的安全管理，保护内部机密信息，确保XXX信息资产安全，规范员工和“第三方”人员在XXX办公区域的行为，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX各部门员工和第三方人员。

## 第三章 术语定义

第三条 办公区域是指XXX内部员工日常办公工作所处的工作区域。

## 第四章职责

第四条 XXX员工在工作期间应遵守本管理规定。

## 第五章办公区域访问控制

第五条 应在工作环境内划定重要办公区域，对重要办公区域的访问应严格限制，未经许可，员工不得擅自进入严格限制的办公区域，如设备室和存储介质室等。

第六条 未经许可和授权，任何人员禁止将办公区域的计算机、笔记本、硬盘、存储介质以及移动介质带离XXX。

第七条 在员工离职时，收回所有员工使用的技术资料和存储介质，以及其它访问权（例

如工卡、办公室钥匙等）。

第八条 接待人员应自觉保守秘密，不得向“第三方”人员透露业务范围之外的技术、商务情况，不随意承诺不在授权范围之外行事，已经承诺和双方达成意向的事宜应当作正式记录。

## 第六章办公环境安全

第十条 员工在下班后桌面上不能有密级纸件文档、磁介质等。下班前，应关闭个人使用设备的电源，并对办公室内公用设备进行检查。员工离开座位超过 30 分钟，桌面上不能有密级相关文档。

第十一条 密级文档应放在抽屉或保密柜内，或交资料

室统一保存。存放机密文件的保密柜必须上锁或设置密码，由专人统一管理。

第十二条 有单独办公室的员工，在离开办公室时必须锁门。

第十三条 当办公室无其他员工时，离开时必须锁门。

第十四条 妥善保管好XXX和个人的贵重物品和仪器，下班后贵重物品和仪器必须存放在保密柜内。保险柜必须上锁或设置密码。

第十五条 员工调离部门或更换办公室时，必须立即交还办公室钥匙以及相关公用设备。

第十六条 维护人员进入办公区域进行设备维修时，应事先和相关部门取得联系，在维修的过程中应有专人进行监督。

第十七条 复印机等设备应由各部门统一管理，员工使用复印机等设备应按有关规定进行，对复印后作废的纸张应及时销毁。

第十八条 指定的义务消防员要积极配合物业部门做好办公室防火安全工作，配合做好大楼消防系统的设备维护工作，熟悉配备的各种灭火器具的使用，并积极配合和接受主管部门对办公区域的安全检查。

## 第七章办公用计算机安全

第十九条 员工应自觉遵守职业道德，有高度的责任心并自觉维护XXX的利益，不利用计算机私自收集、泄漏XXX秘密信息。

第二十条 禁止员工利用XXX网络传播和散布与工作无关的文章和评论，特别是破坏社会秩序的文章或政治性评论。

第二十一条 计算机口令的设置

⑴员工在使用自己所属的计算机时，应该设置开机、屏幕保护和目录共享口令；

用户口令应当同时包含大、小写字母、数字和特殊字符的组合，口令长度要求至少8个字符,不使用弱口令（例如用户名、姓名的拼音等），不得写在纸上或记录于文件中；

口令至少每个季度更改一次，且不得重复。

第二十二条 计算机设备的使用

员工不得私自在办公的计算机设备上装配并使用可读写光驱、磁带机、磁光盘机和 USB 硬盘等外置存储设备；

员工不得私自开启办公计算机机箱，确有需要，应当向相应部门提出申请；

员工不得私自将配备的工作用计算机转借给他人使用。

员工的计算机应设置屏幕保护，一定时间不用后自动加密锁屏。

第二十三条 便携机的使用

在外出办公时，不要使便携式设备处于无人看管状态；

如果物理锁定功能可用，只要便携式设备不在使用时就应该采用该功能；

如果便携式计算机设备被盗，应立即向当地公安机关报案；

不允许将便携式计算机借给无关人员操作，防止程序或数据遭到破坏。第二十四条 移动介质的使用

含有敏感信息的文件存放在移动介质中时，必须加密；

不得在移动介质中长期存贮含有敏感信息的文件，使用完毕后必须及时删除，必要时做低级格式化或者销毁；

不得通过移动介质传播病毒或者恶意程序。

第二十五条 软件使用

员工应安装XXX规定且拥有版权的操作系统和工具软件，不得私自安装与工作无关的应用软件，特别是盗版软件；

员工应当安装、运行XXX规定的防病毒软件并及时升级，对XXX公布的防病毒措施应及时完成，不得私自安装运行未经XXX许可的防病毒软件；

如果员工发现防病毒软件不能有效清除的病毒，应立即报告有关部门，在问题处理前禁止使用感染病毒的文件；

员工不得制造、传播计算机病毒；

员工在安装 Windows 操作系统时，如无特殊需要，不得安装 IIS、TELNET、FTP 等不必要的服务；

员工不得安装、使用黑客工具软件，不得安装影响或破坏XXX网络运行的软件；

对本机上的保密文件，应采取适当的加密措施，并妥善存放。

第二十六条 网络使用

未经允许，员工不能随意更改自己的 IP 地址；

办公网络标准协议为 TCP/IP，非工作需要不得启用任何其它网络协议，如 SPX/IPX，NETBIOS 等；

未经批准，员工不能在XXX内部私自拨号上网；

员工因工作需要在计算机上安装两块或多块网卡并

连接到不同网络设备时，应提出申请由网络管理员负责安装和调试，同时应注意在计算机上不要启动路由网关功能；

员工不应私自更改到网络设备的连接，需要变动时应提出申请，由网络管理员负责更改。

第二十七条 电子邮件系统的使用

员工如收到可疑的电子邮件，不要打开并及时通知安全管理员或本单位等级保护工作联络员处理，以免感染上可能存在的病毒；

外部电子邮件的附件在使用前应进行病毒检查，确保无病毒后才能使用；

在收到来自内部员工发来的含有病毒的邮件，除自己进行杀毒外，还应及时通知对方杀毒；

第二十八条 互联网

员工不应利用XXX上网资源访问与工作无关的站点，特别是淫秽、游戏、反动等类型的网站；

员工不应利用XXX网资源下载与工作无关的文件；

第二十九条 远程拨号（拨入）

远程拨号用户须严格控制，应当由部门负责人确认；

远程拨入XXX内部的员工须使用一次性口令、VPN 技术或采用回拨功能；

远程拨号用户不得将拨入号码告知他人。

第三十条 其它

员工不得私自开设 WWW、FTP、TELNET、BBS 和 NEWS等服务；

员工不得私自设立拨号接入服务；

员工之间不得私下互相转让、借用 IT 资源的账号，如电子邮件账户；

在工作岗位调动或离职时，员工应主动移交各种应用系统的账号；

员工完成应用系统的操作或离开工作岗位时，应及时退出应用系统；

员工离开自己办公计算机时，应将计算机屏幕锁定；

员工如果发现计算机被入侵，应马上通知相关安全部门，按相关规定操作。

## 第八章监督和检查

第三十一条 各部门在办公区域的安全管理上应接受有关职能部门的监督和检查，在计算机的使用上应接受信息安全等级保护工作小组的监督和检查，对在检查中提出的问题要及时整改。

第三十二条 各部门领导及管理员应当对本部门计算机用户进行有效监督和管理，对违反管理规定的行为要及时指正，对严重违反者要立即上报。

第三十三条 安全等级保护工作联络员应当对定期或不定期对各个部门的计算机用户的使用状态进行监督和检查，对违反管理规定的情况要通报批评；对严重违反规定，可能或者己经造成重大损失的情况要立即汇报。

## 第九章持续改进

第三十四条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章附 则

第三十五条 本规定由技术中心制定并负责解释。

第三十六条 本规定自发布之日起施行。

# 九、信息系统信息资产管理规定

## 第一章总则

第一条 为识别XXX的信息资产，指定资产责任人以及确定相关职责，识别资产可接受的使用来对信息资产进行适当保护，防止未授权的访问，特制定本规定。

## 第二章适用范围

第二条 本文件适用于XXX各业务系统相关的信息资产。

## 第三章术语定义

第三条 信息资产：同信息系统相关的对组织有价值的事物，如计算机硬件和软件、数据、服务和文档等。

## 第四章职责

第四条 安全管理员，负责信息资产分类、赋值等，固定资产管理员负责标识、登记以及维修管理。

## 第五章资产分类

第五条 信息资产识别是指按照规定属性对各类信息资产的辨认和区分，包括信息资产识别、分类和登记等项工作。为了便于管理，将资产进行分类，具体分为：

主机设备； 各类承载业务系统和软件的计算机系统及其操作系统，包括安装在服务器上各类应用系统以及构建系统的平台软件（数据库，中间件、群件系统、各商业软件平台等）

网络设备： 包括但不限于二层交换机、负载均衡、光纤转换器、路由器、缓冲服务器、调制解调器、多层交换机，无线 AP、AC、BAS、Hub、RAS、VoIP 网关等构成信息系统网络传输环境的设备；

存储设备：包括但不限于磁带机、磁盘阵列、磁带、光盘、软盘、移动硬盘等

安全设备：VPN 网关、防火墙、内容过滤网关、入侵检测系统、防病毒网关、加密机、安全网闸等构成信息系统信息安全环境的设备，软件；

办公设备；工作站、台式计算机、便携计算机等；

 系统数据、业务数据、XXX信息和技术文档等；

其他设备；打印机、复印机、扫描仪、传真机等。

## 第六章资产分级

第六条 信息资产的安全价值由资产的机密性价值、完整性价值和可用性价值三部分组成。

|  |  |  |
| --- | --- | --- |
| 5 | 很高 | 非常重要，其安全属性被破坏后可能对组织造成非常严重的损失 |
| 4 | 高 | 重要，其安全属性被破坏后可能对组织造成比较严重的损失 |
| 3 | 中等 | 比较重要，其安全属性被破坏后可能对组织造成中等程度的损失 |
| 2 | 低 | 不太重要，其安全属性被破坏后可能对组织造成较低的损失 |

|  |  |  |
| --- | --- | --- |
| 1 | 很低 | 不重要，其安全属性被破坏后对组织造成非常低的损失，甚至忽略不计 |

第七条 根据资产在业务价值和可用性上的赋值等级。

第八条 对所有识别出并进行分类的信息资产，应当进行标识，标识方法可以采用标签、文档标识、数据标识等方法。

## 第七章信息资产标识

第九条 对信息资产进行标识时，应标识信息资产的名称、分类、资产编号、资产管理员、重要级别等信息，根据不同的信息资产类别，标识的内容和方法可以有所不同。

第十条 在资产标识时，不但要有资产的编号，而且要有资产的分级信息和维护人员信息。资产编号原则: 地址-人员-X1-X2-X3说明：地址：表示所在物理位置；人员：表示维护人员信息，包括部门，角色等；X1 为业务平台信息X2 为资产的分类,如主机设备,网络设备等；X3 为资产信息的分级信息。

第十一条 当信息资产的管理者、物理位置、重要级别等等信息发生变更时，需要对相应的标识进行变更，变更记录由各信息资产管理者保存后报技术中心进行复核存档。

第十二条 信息资产的管理者需要维护好自己的所负责的信息的分类清单，并定期回顾更新。

## 第八章信息资产维护

第十三条 技术中心有责任协助固定资产管理员核实和维护信息资产的信息。

第十四条 固定资产管理员应按规定要求对信息资产进行调查，并建立《附件一：信息资产清单》和记录信息资产状况的档案。

第十五条 信息资产属性发生变更时，固定资产管理员要及时对《信息资产清单》进行变更、保存，并报技术中心复核存档。变更包括地理位置变动、信息资产配置信息、补丁信息等变更。

## 第九章闲置报废资产管理

第十六条 闲置资产根据资产类别进行分类归档管理。对任何闲置资产应在资产清单中进行标注。应考虑闲置资产的登记，减少闲置资产丢失的风险；

第十七条 涉及敏感信息或资产级别 3 级以上的闲置资产应在安全管理员处进行备案。对任何可重用的闲置资产中的内容涉及敏感信息，或资产分级 4 级以上，闲置资产中的内容应使其不可重用。要将所有资产分级 4 级及以上的闲置资产存储在安全、保密的环境中；

第十八条 包含有敏感信息的介质或资产级别 3 级及以上要可靠和安全地存储和销毁,对记录纸、设备和介质提供收集和销毁服务，应注意选择合作商；销毁敏感部件或资产级别 3 级及以上要做记录，以便保持审计踪迹。

## 第十章持续改进

第十九条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

第二十条 本文件由技术中心负责制定、解释和修改。

第二十一条 本文件自发布之日起执行。

## 第十一章附则

### 附录一XXX XXXX 系统信息资产清单

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 编号 | 名称 | 机架 | 型号 | 配置 | 服务 | 操作系统 | 内网 IP | 外网 IP | 电源线 | 备注 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

**XXX\*\*\*系统信息资产清单**

# 十、存储介质管理规定

## 第一章总则

第一条 为了保障存储介质的信息安全，对存储介质的标识、传递、访问、保管、销毁等活动提出明确的安全管理规定，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX存储介质安全管理过程。

## 第三章 术语定义

第三条 存储介质：指用于XXX各类业务的电子信息输出、存放的云介质、可修改和不可修改的云磁盘等。

## 第四章组织职责

第四条 系统管理员，负责对存储介质的购买，使用和销毁做授权。对存储介质的购买，使用和销毁必须填写相应的记录表。

第五条 安全管理员，负责对XXX相关存储介质的管理过程进行监督。

## 第五章存储介质标识

第六条 存储介质标志必须置于容易识别的位置，此标签须在存储介质的表面上出现。

第七条 存储介质应该根据不同的分类进行标签，如磁带，磁盘及其它存储介质等有不同的分类标签。

## 第六章存储介质访问

第八条 安装和使用存储介质时必须防止非授权的访问。

第九条 将存储介质给第三方使用，需要系统管理员确认机密信息已经删除。

第十条 必须对所有存储介质的出库和入库及其保持记录进行控制，如要被从库中移出，移出请求应该由一个人完成并且需要相关部门同意，并注明原因和移出时间，介质管理员须在介质清单进行登记。

第十一条 所有含有我院内部信息的存储介质对外部人员都是保密的，严禁我院的员工以及第三方带走；如更换属于合作方保修范围内的损坏介质，需要和合作方签订保密协议，以防止泄漏其中的保密信息。

## 第七章存储介质保管

第十二条 除因工作需求外，禁止任何人持有、复制公司软件，禁止外借或对外复制我院软件。

第十三条 存储介质保存的环境要求（防火、电力、空调、湿度、静电及其他环境保护措施）。

第十四条 对含有机密和绝密信息的存储介质，要存放在保险柜里。

第十五条 必须建立存储目录清单，由相应的管理人负责执行盘点控制的流程，并且存储必须每年盘点一次。当磁带库所有权发生变化时，必须进行一次存储库盘点，并更新介质清单。

第十六条 任何的存储介质盘点与检查出现差异必须报告给部门领导，并且存储介质库的所有介质，包括打开过的空白带、格式化过的、擦除过的、媒体操作装置中的都必须包括在清单盘点中，对存储介质库负责的管理者必须对所有的清单文档签字。

## 第八章存储介质销毁

第十七条 任何计算机存储介质不再用于存储保密信息之前，必须要进行格式化。

第十八条 存储介质的销毁首先要提交销毁申请，经安全管理员确认方可执行销毁，销毁后由介质管理员对介质清单中进行备注。

第十九条 存储介质上删除保密信息后，必须执行重复写操作防止数据恢复。

## 第九章持续改进

第二十条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十章附则

第二十一条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第二十二条 本文件自发布之日起执行。

### 附录一存储介质记录

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 名称 | 介质用途 | 责任人 | 借用人 | 借用时间 | 归还时间 | 借用原因 | 备注 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

### 附录二存储介质销毁申请表

|  |  |
| --- | --- |
| 申请人员： | 联系电话： |
|  | |
| 安全管理员意见：  签字：  年 月 12 日 | |

# 十一、设备安全配置管理规定

## 第一章总则

第一条 为了规范XXX计算机系统管理，包括帐号、密码、补丁、日志以及备份恢复管理过程，提高计算机系统管理水平，保证信息系统安全、稳定、高效运行，特制定本规定。

## 第二章适用范围

第二条 本规定适用于XXX各系统、TCP/IP 网络（生产环境以及办公等非生产环境）安全管理过程，管理对象为医院安全管理员、各系统负责人、管理员及所有使用 IT 设备的员工。

## 第三章术语定义

第三条 账号是指每个可访问系统资源的用户在系统中的标识,可分为应用系统账号、操作系统账号和数据库账号等。

第四条 访问权限是指账号被赋予的可以访问系统资源和使用系统功能的权利。

第五条 特权账号：指对系统具有超级权限的账号，包含但不限于 UNIX/Linux 的 root，WINNT 的 administrators组成员，数据库的 DBA 等用户。

第六条 普通账号：用户用于维护或访问系统，实现日常操作的账号，是最为常见的用户类型。

第七条 补丁是针对某一个具体的系统漏洞或安全问题而发布的专门解决该漏洞或安全问题的小程序，通常称为修补程序。

第八条 日志包括数据中心信息系统中存储的主机系统日志、设备日志和开放平台系统日志等计算机基础环境日志。

第九条 开放平台系统是指安装 UNIX 以及 WINDOWS 系列等操作系统的高低端服务器。

第十条 信息系统密码是指在登录信息系统系统过程中，用于验证用户身份的字符串，以下简称信息系统密码。信息系统密码主要为静态密码、动态密码等。静态密码一般是指在一段时间内有效，需要用户记忆保管的密码。动态密码一般是指根据动态机制生成的、一次有效的密码。信息系统密码主要包括：主机系统（数据库系统）、网络设备、安全设备等系统用户密码；应用系统用户密码；桌面计算机系统用户密码。

第十一条 计算机应用系统备份和恢复工作的规范状况将直接影响系统的恢复程度，目前正在运行的许多应用系统虽然都依照系统本身功能的要求在进行备份，但备份和恢复工作仍不规范，备份和恢复机制（包括但不限于：异地备份、双机热备份、以及源代码和目标码备份、备份周期的合理性、数据的多介质备份）还不完善，再加上各种备份和恢复本身安全机制的限制（如：备份后对正确性、一致性不进行校对）都给应用系统的恢复工作造成各种影响，直接威胁应用系统的安全性和完整性，因此特制定计算机应用系统备份的管理规定，以便在遇到诸如：突发停电、机器故障以及其他不可预测的外力影响时能及时恢复应用系统的使用。

## 第四章组织职责

第十二条 各系统管理员负责相关系统管理，配合安全管理员进行信息系统安全管理。

第十三条 安全管理员，负责对XXX信息系统安全管理过程进行监督。

第十四条 XXX技术中心负责对用户帐号权限的安全管理工作。

## 第五章账户管理

第十五条 对系统的访问必须经过授权，任何人不得在未经授权的情况下在系统中运行未经审批的程序。授权可以通过书面文件，或通过员工按岗位的分工等方式实现。

第十六条 各系统应采用用户名和密码认证方式实现登录控制，对系统的访问应使用唯一的帐号和口令。

第十七条 各系统中不应建立共享帐号，每个帐号都与唯一的用户相对应。拥有帐号的用户不得随意将帐号交于他人使用。

第十八条 帐号权限的分配应遵循满足需求的最小授权原则, 即为用户分配权限时, 以其能进行系统管理、操作的最小权限进行授权，避免为其分配无关的或更大的权限。

第十九条 有关用户登陆和帐号权限管理的相关操作在系统中要留有日志,日志至少保留 3 个月。

第二十条 创立新用户角色或对用户组或用户角色定义进行修改时，应考虑不相容职责分工原则，例如操作人员与审核人员的分离、开发人员与维护人员的分离等。

第二十一条 当员工工作调动或离职时，其在系统中的帐号应立即撤销，不得继续将帐号分配给他人使用。

第二十二条 开发人员平时不得使用生产环境中系统帐号。如需使用，则必须向安全管理员提出申请,经安全管理员同意后,由系统管理员临时为其开启一个临时帐号 .开发人员在访问生产系统时必须由系统维护人员对其访问进行监督，在访问结束后及时删除帐号或更改口令,并对操作日志进行审阅。第二十三条 如果系统中存在第三方厂商人员使用帐号的情况，应和第三方厂商签订相关的安全保密协议，以合理确保第三方厂商能够执行XXX安全管理要求和职责不相容要求.如果外部人员需要通过远程登录访问对系统进行操作及更新，向安全管理员提出申请（附录一、XXX业务系统临时帐户申请表），由相关系统管理员临时开通远程登录功能。在操作完成后，系统管理员应及时终止远程登录。

第二十四条 对于部分因系统接口原因在系统中预设的用户帐号，应对接口程序、脚本或相关设置进行加密或实施访问控制，以防止未经授权的访问。

第二十五条 对于各系统应使用分级管理，设立特权帐号以及临时使用的普通帐号，并且对帐号分不同安全等级进行管理，定期检查用户的帐号及其权限，重点检查有特权的帐号是否存在特权时限过期。

第二十六条 由系统管理员对所有帐户进行登记（附录二、XXX业务系统帐户清单），并根据需要或定期进行审查、更新。

第二十七条 业务系统的特权帐号由负责相关工作的系统管理员持有，并妥善保存。

第二十八条 系统因维护需要使用特权帐号，但系统管理员因特殊原因不能够在现场实施特权帐号登录操作，则系统管理员可以指定一个临时使用人使用特权帐号处理问题，任务完成后，系统管理员应立即更新相应的特权帐号密码以收回特权帐号的使用权限。

第二十九条 服务提供商或产品厂家技术人员等第三方人员对系统进行维护时，如果需要使用特权用户，系统管理员可以通过设置临时口令的方式给第三方人员授权使用特权帐号，当授权到期后立即通过更改特权帐号口令收加特权帐号。

第三十条 相关系统管理员离职后，应当立即更新其所持有的特权帐号密码。

第十三一条 系统管理员根据“最少权限”的原则，审批普通帐号和权限的申请，在得到相关部门复审后，系统管理员可以执行帐号与权限的操作。

第三十二条 系统用户离职或岗位调整，该用户直接领导必须通知系统管理员，系统管理员进行用户信息调整并及时更新帐户清单。

第三十三条 用户离职或岗位调整后，该用户直接领导未通知系统管理员的，由于该用户造成的损失由该用户的直接领导负责。第三十四条 普通用户的日常维护工作由系统管理员负责。

第三十五条 帐号口令拥有者必须严格确保口令的安全保密性。一旦有迹象表明口令可能被泄露，用户必须立即修改口令。

第三十六条 系统中的帐号口令应避免使用弱口令.口令长度不得低于 8 位，须由数字、大小字母以及特殊字符组成,并至少 3 个月进行更新。

第三十七条 帐号的初始口令应以安全途径告知帐号使用者.帐号使用者在首次登录系统时应立即修改帐号口令。

第三十八条 用户忘记口令时，管理员必须在对该用户进行适当的身份识别后才能向其提供临时口令。

第三十九条 口令在系统中保存或传输时,必须采取安全措施以保证帐号的安全性,例如对口令进行加密等. 除非可以安全保管，否则不得将口令记录在纸张等一切可视介质上。

第四十条 当程序内的帐号密码需要保存在配置文件里时，文件属性应置为不可读,并且只能由对应用程序访问。

第四十一条 各业务系统安全管理员负责检查监督生产系统的特权账户口令管理，至少 3 个月进行 1 次检查。

## 第六章系统密码管理

第四十二条 系统要求密码管理

XXX所使用的操作系统、业务系统、数据库、网络设备等均需要支持基于帐号的访问控制功能；

所有需要使用口令的应用软件、业务软件都需要对口令文件提供妥善的保护。

第四十三条 帐号申请原则

只有授权用户才可以申请系统帐号；

任何系统的帐号设立必须按照规定的相应流程规定进行；

员工申请帐号前应该接受适当的培训，以确保能够正常的操作，避免对系统安全造成隐患；

帐号相应的权限应该以满足用户需要为原则，不得有与用户职责无关的权限；

对于确因工作需要而必须申请系统帐号的XXX外部人员，则必须经部门领导批准，且有XXX正式员工作为安全责任人，如果需要接触XXX秘密信息，必须通过技术中心审批并且签署保密协议；

任何系统的帐号必须是可以区分责任人，责任人必须细化到个人，不得以部门或个人组作为责任人。

第四十四条 公用帐号

系统应当严格限制开设公用帐号，一般情况下公用帐号不得具有访问保密信息和对系统写的权限；

公用帐号应该设立责任人，负责帐号的正常使用及维护。

第四十五条 匿名帐号

匿名帐号只被允许访问系统中可公开的且对XXX有益的资源，不得访问任何内部公开及以上秘密等级的资源；

对匿名用户对系统的访问必须有详细的记录。

第四十六条 口令的生成

系统帐号分配时必须同时生成相应的口令，并且与帐号一起传送给用户；

用户在接受到帐号和口令后，必须马上修改口令，任何时间都不得存在没有口令的帐号，除非该帐号已经失效；

对于系统的帐号验证只有口令作为证据的系统，如果帐号名由确定的且公开的规则产生的，则口令不应当为公开的口令；

⑷管理员在传递帐号和口令时，应当采取加密或其他安全的传输途径，以保证口令不会被中途截取。

第四十七条 口令设立的原则

帐号口令必须是具有足够的长度和复杂度，使口令难于被猜测；

帐号口令必须是在必要时间或次数内不循环使用；

帐号的各个口令之间应当是没有直接联系的，以保证不可有以前的口令推知现在的口令；

帐号的前后两个口令之间的相同部分应当尽量减少，减低由前一个口令分析出后一个口令的机会；

帐号的口令不应当取有意义的词语或其他符号，如使用者的姓名，生日或其它易于猜测的信息。

第四十八条 口令的最低标准

帐号口令长度不得低于 8位，最近 5 个口令不可重复，口令中必须包含大写字母，小写字母，特殊字符和数字四种中的三种。

第十四九条 帐号的使用

任何帐号的使用人只限于申请帐号过程中声明的使用人使用，禁止其他人使用此帐号；

帐号系统正式使用前，必须更改原来系统中的缺省帐号的所有口令，以保证正式环境的安全；

帐号使用人在使用的过程中，不得使用帐号访问与自己工作无关的资源。

第五十条 帐号的权限变更

帐号使用人在工作职责发生转变，造成现有职责与现有的在系统中的职责不同时，应当申请权限的修改；管理员发现用户具有工作不需要的权限，可以直接停止多余的权限；

帐号使用人在工作职责发生转变，而不再需要使用系统资源的情况下，应当申请关闭帐号；对不能关闭的帐号则需要转移帐号的责任人。

第五十一条 口令的修改

帐号的使用人应当定期修改帐号口令，修改口令的间隔应小于本标准的相关规定，对于本标准没有规定的用户，其间隔应当小于 3 个月；

帐号用户必须在管理员要求更改口令时进行更改口令；如果用户拒绝配合，管理员可以在通知用户及其主管后，关闭用户的帐号，以保证系统的安全；

帐号用户丢失或遗忘口令，必须通过规定的流程向管理员申请初试化口令，用户在接到回执后，应马上更改口令；

帐号用户要求口令修改的方式必须是可以确保用户身份的，且管理员必须有记录；

管理员不可在没有用户申请的时候私自更改用户帐号的口令，除非XXX技术中心需要；

系统的超级管理员帐号的口令属于系统最高机密，应该严格限定使用范围；其他人员确因工作需要而使用超级管理员帐号和口令的，应当向超级管理员帐号和口令的责任人申请口令，并在完成操作后，由责任人更改口令。

第五十二条 帐号的取消

用户如果因职责变动而离岗，不再需要系统权限且无须将帐号移交给其他责任人，其原岗位主管应当申请帐号的销户，由管理员取消其权限；

用户离职后，管理员应当关闭用户在系统中的所有权限。

第五十三条 密码口令的管理

不能将密码口令以纸质介质或明文电子数据保存，不能通过电子邮件传输；

不能使用缺省设置的密码；

不能将密码告诉别人；

若发现系统的密码泄漏了，必须立即更改；

不能共享超级用户的口令，使用用户组或适当的工具如 su；

所有系统集成商在施工期间设立的缺省密码在系统投入使用之前都要删除；

密码要以加密形式保存，加密算法强度要高，加密算法要不可逆；

在输入时密码不能显示出来；

系统应该强制指定密码的策略，包括密码的最短有效期、最长有效期、最短长度、复杂性等；

除了系统管理员外，一般用户不能改变其它用户的口令；

如果需要特殊用户的口令（如 UNIX 下的 Oracle），要禁止通过该用户进行交互式登录；

强制用户在第一次登录后改变口令；

在要求较高的情况下可以使用强度更高的认证机制，例如：双因素认证；

可能的话，可以使用自己密码生成器帮助用户选择口令；

要定时运行密码检查器检查口令强度，对于保存机密和绝密信息的系统应该每周检查一次口令强度；其它系统应该每月检查一次。

第五十四条 信息系统用户的责任与义务

⑴所有用户有义务确保自己的口令的安全，系统帐号与口令不泄漏给他人，同时避免使用弱口令；

⑵对于使用便携式计算机的用户，应设置开机 BIOS 口令；

⑶使用远程登陆的用户，确保不将口令保留在计算机上；

⑷不将信息系统中使用的帐号和口令用于其他个人应用；

⑸任何人不得公开其本人或他人口令的全部或部分，除非这种行为不会影响系统帐号的安全性；

⑹严禁任何人通过任何手段非法取得他人帐号和口令进入系统，对违反者应当进行严厉制裁，直至追究法律责任；

⑺任何人不得将其帐号的口令告之无权使用此帐号的人，如果用户此种行为导致其他人用此帐号造成对XXX信息系统的影响，帐号持有人和造成影响的行为的实施人负有相同的责任；

⑻严禁任何人利用系统安全漏洞访问其权限之外的资源，一经发现，立即严惩。

第五十五条 系统管理员的责任与义务

⑴确保除匿名帐号外，所有系统用户都必须有口令；

⑵定期审计，检查系统用户的数量和权限；

⑶确保系统和网络设备无默认帐号和口令；

⑷确保关键应用服务器启用口令强制策略；

⑸对用户进行口令安全培训；

⑹建议同一个管理员在不同主机上使用不同的帐号和口令。

第五十六条 XXX内部人员的信息系统帐号的开户/权限变更按照以下流程进行：

⑴首先由用户提出书面申请，详细列出所需权限，由其部门领导审批其申请的权限是因为工作需要；

⑵如果用户申请系统规定的需要高级主管或其他部门主管审批的权限则需要其他部门或高级主管审批；

⑶如果有必要，由系统中业务部门的负责人员进行用户的要求是否合理的审批；

⑷然后由安全负责人员审核其安全性，相应负责人员进行开户操作，在以上各审批人的审批环节中，如任何一个审批人不同意该申请，则退回用户的申请。

第五十七条 非XXX人员的信息系统中的开户，除非技术中心有其他规定，否则均按照以下流程进行：

⑴由接口部门的责任人代替非XXX人员申请，并明确指明责任；

⑵由非XXX人员的接口部门或以上部门领导进行审批；

⑶如需要，由其他部门领导审批；

⑷安全管理人员进行审批、备案；

⑸业务负责人审批申请的合理性；

⑹相应负责人员进行开户；

⑺在以上各审批人的审批环节中，如任意一个审批人不同意用户的申请，则退回用户的申请；

⑻如有明文规定的非XXX人员的开户，按照具体规定执行。

第五十八条 用户因职责变动，而不需要使用信息系统的资源，应当立即销户，XXX内部人员的帐号的销户流程如下：

⑴用户主管提出申请；

⑵安全控制人员审批并执行（离职人员的帐号由安全控制办人员直接处理）。

第五十九条 非XXX人员的帐号停止使用后，责任人应当负责提出销户，销户流程如下：

⑴帐号的责任人提出申请；⑵接口部门的主管审批；

⑶技术中心审批并备案；

⑷安全管理人员操作。

第六十条 例外情况

⑴安全管理人员在因系统安全原因或紧急情况下，在得到主管部门允许的情况下，不经过以上流程而执行帐号操作；

⑵因系统升级或迁移等情况下，可以在得到相应部门认同的情况下，直接操作而不经过本流程。

## 第七章补丁管理

第六十一条 安全管理员和各系统管理员负责从正式渠道获取安全补丁，正式渠道包括企业下发的和产品厂商提供的，不建议使用从网站下载的安全补丁，并负责对安全补丁进行完整性校验，确保获取的安全补丁软件未被修改和可用。

第六十二条 跟踪信息系统的补丁信息，跟踪手段包括但不限于：

⑴定期跟踪信息资产厂家的补丁发布网站，或者最新的补丁信息，最少每月查询一次。

⑵定期通过安全漏洞扫描器扫描信息资产的漏洞缺失情况，最少每季度扫描一次。

⑶同相关信息资产厂家建立补丁通告协议

第六十三条 补丁在发布之后的两周之内要获取补丁信息。

第六十四条 购买新系统和设备的时候，进行补丁检查，确保厂家已经安装了较新的补丁。

第六十五条 业务系统以及所属基础平台相关系统补丁加载前必须进行补丁测试。

第六十六条 补丁测试必需在测试环境中进行，测试过程和测试结果要保留记录备查，测试没有通过的补丁不得在生产系统中加载。

第六十七条 不具备测试条件的补丁加载，要制定并提交加载过程风险规避方案，确保加载不成功时的系统恢复。

第六十八条 补丁测试的内容包括补丁安装测试、补丁功能性测试、补丁兼容性测试和补丁回退测试：

⑴安装测试主要测试补丁安装过程是否正确无误，补丁安装后系统是否正常启动。

⑵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。

⑶补丁兼容性测试主要测试补丁加载后是否对应用系统带来影响，业务是否可以正常运行。

⑷补丁回退测试主要包括补丁卸载测试、系统还原测试。

第六十九条 各系统或设备管理员负责组织进行补丁测试工作，安全管理员负责组织办公用机的补丁测试工作，重要生产系统进行补丁测试工作必须安排相关厂商进行配合。

第七十条 各系统或设备管理员需要把补丁测试结果提交给各科室负责人进行审核，并在《业务系统补丁安装登记表》中进行登记，审核通过后可以进行补丁加载。

第七十一条 补丁安装完成后，各系统或设备管理员必需查看系统信息，确保安全补丁已经成功加载。

第七十二条 对于生产环境的服务器，必须对加载补丁后的系统按照计划和验证方案进行严格的测试验证，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。

第七十三条 华泰办公个人电脑在补丁安装前必须做备份，确保补丁可回退的措施。

第七十四条 补丁加载后的一周内，各系统或设备管理员必须加强对系统性能和事件进行密切的监控。

第七十五条 对系统补丁的加载进行归档处理，备份加载过的补丁包，对每一个需要进行补丁管理的重要信息资产（服务器操作系统、数据库、网路设备、安全设备、应用系统等）建立补丁加载记录，对于没有加载的补丁标注原因和相应的防范措施。

## 第八章日志管理

第七十六条 日志不能被无关人员随意察看；日志本身需要保持完整性，不能被非授权人员更改；日志需要保持可用性，要做备份，以便审计时使用。

第七十七条 日志需至少包括以下内容：

⑴用户帐号；

⑵登录和退出的日期和时间；

⑶尽可能的识别出终端的身份代号或地址；

⑷记录有相关系统访问成功和失败的登录日志；

⑸成功和拒绝处理的数据和其它资源访问登录的相关记录。

第七十八条 为了统一日志管理，便于审计，应当建立时间同步服务器，对重要系统日志进行时间同步。

第七十九条 应当建立日志服务器，日志服务器使用大容量磁盘，实施对所有日志进行收集、保存，日志传送可以通过 SNMP，SYSLOG 等方式。

第八十条 日志维护管理的结果必须每周进行检查，如发现有可疑的滥用或安全性事故的情况发生，则及时对问题进行分析和跟踪；对影响较大的错误日志必须及时向相关部门负责人汇报。

第八十一条 业务系统运行维护人员应每 6 个月对运行日志和审计数据进行分析，以便及时发现异常行为。

第八十二条 主机系统日志由操作系统日志和数据库日志组成。

第八十三条 对主机日志的访问权限进行控制，并打开审计选项，以防止非法访问。

第八十四条 系统管理员应对生产环境的各类主机日志进行备份，涉及到重要或机密数据应当备份到存储介质上进行异地保存，主机系统日志保留 6 个月；数据库管理员对数据库进行管理，日志保留期限为 6 个月。

第八十五条 各部门如需查阅主机系统日志，应按照XXX有关信息系统变更管理的要求提交变更申请，由系统管理员或数据库管理员调出指定的主机日志到非生产环境，查阅完成后，在非生产环境上删除。

第八十六条 应当在业务系统服务器上进行配置或运行脚本，将每日日志集中发送至日志服务器。

第八十七条 对业务系统日志的访问权限进行控制，并打开审计选项，以防止非法访问。

第八十八条 日志文件在日志服务器上集中保存；日志保留期限为 6 个月。

第八十九条 各部门如需查阅业务系统日志，应向本部门负责人或各组负责人提出申请，相关负责人同意后，由各系统管理员负责相关日志的收集，通过可以查询或保留的方式进行发送，如邮箱；查阅完成，各申请人员必须及时对日志进行删除。

第九十条 设备日志主要是由防火墙、路由器、交换机、负载均衡设备、通信设备等产生的日志。

第九十一条 应当在设备上进行配置或运行脚本，将每日日志集中发送至日志服务器。

第九十二条 对设备日志的访问权限进行控制，并打开审计选项，以防止非法访问。

第九十三条 日志文件在日志服务器上集中保存；日志保留期限为 6 个月。

第九十四条 各部门如需查阅设备日志，应向本部门负责人或各组负责人提出申请，相关负责人同意后，由相关管理员负责相关日志的收集，通过可以查询或保留的方式进行发送，如邮箱；查阅完成，各申请人员必须及时对日志进行删除。

## 第九章备份管理

第九十五条 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。

第九十六条 业务系统管理人员或其授权人员应填写

《附录一：业务系统备份数据清单》，并由业务系统主管审批签字，以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。

第九十七条 数据备份采用 0 级备份或增量备份。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。

第九十八条 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。

第九十九条 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。

第一百条 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。第一百零一条 操作系统备份要求：

⑴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。

⑵ 操作系统应每半年至少备份一次。

⑶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。

⑷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。

⑸ 操作系统层的备份由系统管理员负责实施。

⑹ 所有操作系统层的备份完成后应至少保留三个月。

第一百零二条 数据库备份要求：

⑴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。

⑵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。

⑶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。

⑷数据库数据文件应每周至少备份一次。

⑸数据库归档日志应每天进行增量备份。

⑹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。

⑺ 数据库层备份由数据库管理员负责实施。

⑻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。第一百零三条 应用系统备份要求：

⑴应用系统层备份包括应用系统程序文件和日志文件。

⑵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。

⑶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。

⑷应用系统备份由应用系统管理员负责实施。

⑸所有的应用系统备份应至少保留三个月。

第一百零四条 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。

第一百零五条 业务系统负责人或团队经理指派相应备份管理人员对本地备份数据情况进行定期的检查，并填写《附录二：本地备份登记记录》，相关业务系统主管应每月对《本地备份登记记录》签字审核。

第一百零六条 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。

第一百零七条 备份管理人员应及时对冷备介质进行异地存放，并填写《附录三：异地备份登记记录》，业务系统主管应每月对《异地备份登记记录》签字审核。

第一百零八条 备份管理人员应制定详细可操作的备份恢复操作方案，并由业务系统主管审批签字。

第一百零九条 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。恢复测试完毕后，及时填写《附录四：备份恢复测试记录》。

第一百一十条 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，并在更换后填写《附录五：备份介质更换记录》，相关业务系统主管应每半年对《备份介质更换记录》签字审核一次．

第一百一十一条 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。

第一百一十二条 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。

第一百一十三条 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。

第一百一十四条 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。

第一百一十五条 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。

第一百一十六条 安全管理员应每月对备份介质进行审核并签字确认。

## 第十章恢复管理

第一百一十七条 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，获得技术中心负责人的批准后才可实施。

第一百一十八条 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。

第一百一十九条 数据恢复必须严格按照操作手册执行，出现问题时由技术中心相关人员进行现场技术支持。

第一百二十条 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。

第一百二十一条 由数据备份人员根据XXX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。

第一百二十二条 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。

第一百二十三条 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。

## 第十一章持续改进

第一百二十四条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第十二章附则

第一百二十五条 本文件由技术中心负责制定、解释和修改。

第一百二十六条 本文件自发布之日起执行。

|  |  |
| --- | --- |
| 申请人员： | 联系电话： |
| 申请原因、期限及用途： | |
| 系统管理员意见同意  签字：  年 月 日 | |

### 附录一XXX业务系统临时帐户申请表

XXX业务系统临时用户申请表

日期：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 帐户名称 | 帐户类别 | 所属平台系  统 | 用途 | 使用人  员 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

### 附录二XXX业务系统帐户清单

XXX业务系统帐户清单

日期：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 系统名称 | 补丁名称 | 补丁安装时间 | 安装申请人 | 安装审批人 | 简要描述  补丁更新  原因 |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

### 附录三XXX业务系统补丁安装登记表

XXX统一认证授权管理后台业务系统补丁安装登记表

日期：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 备份恢复操作方案 | | | | | | |
| 业务系统名称 | |  | | | | |
| 序号 | 数据名称 | 操作人员 | | 联系方式 | 备份恢复操作步骤 | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
|  |  |  | |  |  | |
| 备注： | | | | | | |
| 业务系统主管审批签字 | | |  | | 签字日期 |  |

编号：

### 附录四XXX业务系统备份恢复操作方案

### 附录五XXX业务系统备份恢复测试记录

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 备份恢复测试记录 | | | | | | | | |
| 业务系  统名称 |  | | | | | | | |
| 备份介  质编号 | 备份数  据名称 | 介质  类型 | 介质存  放地点 | 测试方案 | 测试结果 | 后续工作 | 测  试  人 | 测试  日期 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
| 备注： | | | | | | | | |

编号：

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 备份介质更换记录 | | | | | | | | | | |
| 备份数据  名称 | 存放地点 | 原备份介质 | | | 新备份介质 | | | | 更换  人签  字 | 更换  日期 |
| 介质编号 | 介质  类型 | 数  量 | 介质编  号 | | 介质  类型 | 数  量 |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
|  |  |  |  |  |  | |  |  |  |  |
| 备注：业务系统主管每半年审核一次。 | | | | | | | | | | |
| 业务系统主管审核  签字 | |  | | 签字日  期 | |  | | | | |

编号：

### 附录六XXX备份介质更换记录

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 本地备份登记记录 | | | | | |
| 业务系统名称 | |  | | | |
| 数据名称 | 备份方式 | 备份状态 | 备份人签字 | | 备份日期 |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
|  |  |  |  | |  |
| 备注： | | | | | |
| 业务系统主管审核签字 | |  | 签字日期 |  | |
| 审核意见 | |  | | | |

### 附录七XXX本地备份登记记录

编号：20181018

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 本地备份介质使用记录 | | | | | | |
| 业务系统名称 | |  | | | | |
| 介质编号 | 数据名称 | 姓名 | 借用日期 | 归还日期 | 使用原因 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 审核意见 | |  | | | | |
| 安全管理员审核签字 | |  | | 签字日期 |  | |
| 审批意见 | |  | | | | |
| 主管部门领导审批签字 | |  | | 签字日期 |  | |

### 附录八本地备份介质使用记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 本地备份介质授权记录 | | | | | | |
| 业务系统名称 | |  | | | | |
| 介质类型 | 数据名称 | 姓名 | 单位 | 职务 | 联系电话 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 审核意见 | |  | | | | |
| 业务系统主管审核签字 | |  | | 签字日期 |  | |
| 审核意见 | |  | | | | |
| 安全管理员审核签字 | |  | | 签字日期 |  | |
| 审批意见 | |  | | | | |
| 主管部门领导审批签字 | |  | | 签字日期 |  | |

### 附录九本地备份介质授权记录

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 业务系统备份数据清单 | | | | | | | | |
| 业务系统  名称 | |  | | | | | | |
| 序  号 | 数据  名称 | 保 存  期限 | 操作方式  （ 手 工  /自动） | 备份  方式 | 备份  周期 | 操作  人员 | 联系  方式 | 备份操作步骤 |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

### 附录十业务系统备份数据清单

|  |  |  |  |
| --- | --- | --- | --- |
| 备注： | | | |
| 业务系统主管审  批签字 |  | 签字日期 |  |
| 主管部门领导审  批签字 |  | 签字日期 |  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 异地备份登记记录 | | | | | | | | |
| 业务系统名称 | |  | | | | | | |
| 介质编号 | 数据名称 | 介质类型 | 数量 | 存放地点 | | 备份人签字 | | 备份日期 |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
|  |  |  |  |  | |  | |  |
| 备注：业务系统主管每月审核一次。 | | | | | | | | |
| 业务系统主管审核签字 | |  | | | 签字日期 | |  | |
| 审核意见 | |  | | | | | | |

### 附录十一异地备份登记记录

编号：20181022

### 附录十二异地备份介质恢复测试记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 异地备份介质恢复测试记录 | | | | | | |
| 介质编  号 | 介质类  型 | 备份数据名  称 | 存放地点 | 测试结果 | 测试人  签字 | 测试日  期 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 备注： | | | | | | |

编号：2018101801

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 异地备份介质使用记录 | | | | | | |
| 业务系统名称 | |  | | | | |
| 介质编号 | 数据名称 | 姓名 | 借用日期 | 归还日期 | 使用原因 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 安全管理员审核签字 | |  | | 签字日期 |  | |
| 审批意见 | |  | | | | |
| 主管部门领导审核签字 | |  | | 签字日期 |  | |

### 附录十三异地备份介质使用记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 异地备份介质授权记录 | | | | | | |
| 业务系统名称 | |  | | | | |
| 介质类型 | 数据名称 | 姓名 | 单位 | 职务 | 联系电话 | 备注 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
| 审核意见 | |  | | | | |
| 业务系统主管审核签字 | |  | | 签字日期 |  | |
| 审核意见 | |  | | | | |
| 安全管理员审核签字 | |  | | 签字日期 |  | |
| 审批意见 | |  | | | | |
| 主管部门领导审批签字 | |  | | 签字日期 |  | |

### 附录十四异地备份介质授权记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 基本信息 | | | | | | |
| 加固日期 | |  | | | | |
| 加固人员 | |  | | | | |
| 设备所属系统 | |  | | | | |
| 设备所属等级 | |  | | | | |
| 设备物理位置 | |  | | | | |
| 正式域名/主机名 | |  | | | | |
| 设备 IP 地址 | |  | | | | |
| 操作系统及版本号 | |  | | | | |
| 备注： 数据库,中间件 | | | | | | |
| 序列 | 操作名称 | | 添加/删除/修改 | 操作步骤 | 回退办法 | 完成情况 |
|  |  | |  |  |  |  |
|  |  | |  |  |  |  |
|  |  | |  |  |  |  |
|  |  | |  |  |  |  |
|  |  | |  |  |  |  |
| 6 |  | |  |  |  |  |

### 附录十五主机操作日志

操作人员:\_\_\_\_ \_\_\_\_\_\_\_\_\_

日期:\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_

# 十二、防病毒管理规定

# 第一章总则

第一条 为加强对XXX信息系统的服务器和终端 PC 机的防病毒管理，保证信息系统稳定快速安全运行，提高全体员工的防病毒意识，落实全体员工的防病毒责任，制定本规定。

## 第二章适用范围

第二条 本标准规定了XXX各系统对计算机病毒防治的管理内容。

第三条 本标准适用于XXX所有员工计算机设备的防病毒要求。

## 第三章术语定义

第四条 计算机病毒：计算机病毒是人为蓄意编制的一种寄生性的计算机程序。它能在计算机系统中生存，通过自我复制来传播，在一定条件下即被激活，从而给计算机系统造成一定损害甚至严重破坏，有些病毒还能窃取计算机设备中的重要信息。

## 第四章组织职责

第五条 计算机病毒的防治工作由XXX技术中心负责，承担制定各类相关的管理规定，研究各类计算机病毒防治技术，并牵头实施、负责检查、考核及奖惩。

⑴监管XXX防病毒情况；

⑵监督防病毒产品的部署和使用；

⑶组织计算机防病毒教育和培训；

⑷负责防病毒规定的制定和维护；

⑸对计算机的防病毒情况进行检查；

⑹对用户上报的病毒追踪其根源，查找病毒传播者；

⑺为XXX提供相关重大突发性病毒的预警和发布。

第六条 安全管理员组织职责

⑴负责与防病毒和专业安全厂商保持联系；

⑵监督和审核XXX防病毒情况。

⑶负责维护和管理防病毒服务器；

⑷配置查杀策略和升级策略；

⑸每天早晨检查防病毒服务器病毒定义更新；

⑹每周五早晨检查网络中病毒的发作情况；

⑺负责计算机病毒预警发布；

⑻接受用户的计算机病毒报告，并进行相应的诊断、分析、处理和记录备案；

⑼每月填写《防病毒系统运行情况报告》，提交等级护领导小组。

第七条 系统管理员组织职责

⑴在所管理计算机上发现可疑的计算机病毒现象时及时向网络管理员报告，配合网络管理员进行病毒的清除和处置；

⑵ 服务器和个人 PC 的防病毒软件的安装。

## 第五章防病毒管理内容

第八条 XXX生产环境各系统所使用的计算机病毒产品，由XXX统一购买和发放。各系统管理员按安全管理员规定在指定地点下载使用防病毒软件。

第九条 各系统应落实专人负责本部门的计算机病毒安装查杀工作，并报XXX信息部备案，人员发生变更及调整时应及时上报信息部办理变更登记。

第十条 信息部通知各系统（部门）进行计算机防病毒产品的安装及升级办法，并指导升级工作，防病毒软件中心应设置自动扫描工作，并由安全管理员确认扫描结果。

第十一条 及时检查防病毒软件以及病毒库的升级更新情况。

第十二条 订购专业安全厂商的安全通告服务，及时获取病毒预警信息。

第十三条 对于新入网的终端，要先安装防病毒软件。

第十四条 定期对全网进行病毒检测，进行全网的病毒综合分析和报告，并由安全管理员确认扫描结果，发现问题立即处理并报告。

第十五条 在所管理计算机上发现可疑的计算机病毒现象时及时向安全管理员报告，配合按管理员进行病毒的清除和处置。

第十六条 对于不能立即解决的病毒问题，信息部及时组织协同相关的技术和业务人员进行跟踪解决，并及时联系防病毒厂商，在问题解决前尽快采取相应措施阻止事件进一步扩大。

第十七条 对于因计算机病毒引起的计算机信息系统的瘫痪、程序和数据严重破坏等重大、较大事故，应做好现场保护工作，参照《XXX信息系统应急预案管理规定》进行汇报和处置。

## 第六章防病毒应用规定

第十八条 各系统管理人员禁止私自安装非法软件和卸载安装的防病毒软件。

第十九条 各系统管理员禁止运行未经审核批准的软件，对于外来的（如：网络下载、可移动磁盘等介质）程序和文档，应在运行或打开前进行计算机病毒的检测和清除。

第二十条 使用 web 方式接收电子邮件时，不得随意打开来历不明或可疑的电子邮件。使用邮件系统接受带有附件的邮件时，要开启防病毒软件的邮件接收监控功能。

第二十一条 各系统员工在遇到或怀疑发生防病毒软件不能查杀的病毒事件时，应第一时间报告到信息部监管部门。第七章惩罚制度。

## 第七章惩罚制度

第二十二条 对故意制造、传播计算机病毒的，触犯国家有关法律或规定的人员由相关部门依照国家有关法律、法规进行处罚。

第二十三条 对于违反本标准规定而造成计算机系统瘫痪，严重影响股票交易或其他生产系统，产生严重后果的，视情节轻重按XXX有关规定对责任人及其所在部门实施处罚。

第二十四条 本标准执行情况列入各系统（部门）的XXX信息化单项考核中。

## 第八章持续改进

第二十五条 为了保证本规定的时效性、可用性，必须根据相关审核规定进行评审和修订，修订后重新发布。

## 第九章附则

第二十六条 本文件由技术中心负责制定、解释和修改，XXX过去制定和颁布的有关规定与本文件不一致的，以本文件为准。

第二十七条 本文件自发布之日起执行。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 查杀时间 | 查杀人 | 查杀记录 | 备注 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

### 附录一人工查杀病毒记录

# 十三、沟通与合作

## 第一章总则

为加强广州XXX对外和对内的沟通，避免沟通不畅导致的生产故障或处理效率降低。

## 第二章适用范围

本规范适用于XXX对外各合作伙伴和内部各部门的沟通管理。

## 第三章组织职责

第一条，为更高效的处理信息安全问题，应加强与外部信息安全专家、安全医院、安全组织的合作与沟通，通过聘请信息安全专家和外部顾问成员，指导广州XXX信息安全建设，参与安全规划和评审。专家和外部顾问负责对信息安全重要问题的决策提供咨询和建议。

第二条，广州XXX信息安全领导小组应保持与国家主管机关、监管机构和上级信息安全主管单位的沟通顺畅。

第三条应能够与广州XXX网络链路提供机构、信息系统托管运维机构、信息系统的硬件设备、软件设备提供商保持合作，确保在出现各类安全问题时能够沟通顺畅。

第四条，应能够及时跟踪国内外各类信息安全信息，了解相关信息安全态势，及时收取与广州XXX相关的脆弱性、建议和补丁信息。

第五条，信息中心安全管理员应及时维护《广州XXX常用信息安全组织机构信息表》（附表2）和安全顾问相关文档（附表3）。

第六条，广州XXX信息安全领导小组办公室应与广州XXX有关单位、信息中心有关部门建立沟通、合作机制，定期组织相关单位、部门召开内部协调会议，信息安全领导小组也应定期召开例会，协调指导信息安全工作的实施。

第七条，信息中心资产管理负责维护内部安全工作会议文件或会议记录（附表4）。

## 第四章附则

XXX信息安全小组联系表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 姓名 | 单位 | 联系方式 | | |
| 职务 | 手机号码 | 电话号码 | 传真 |
| 组长 |  |  |  |  |  |
| 副组长 |  |  |  |  |  |
| 成员 |  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
| 日常工作联系人 |  |  |  |  |  |

XXX对外合作伙伴联系方式表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **合作单位名称** | **联系人** | **联系方式-电话** | **联系方式-邮件** | | **合作内容** | **备注** |
| 1 |  |  |  |  | |  |  |
| 2 |  |  |  |  | |  |  |
| 3 |  |  |  |  | |  |  |
| 4 |  |  |  |  | |  |  |
| 5 |  |  |  |  | |  |  |
| 6 |  |  |  |  | |  |  |
| 7 |  |  |  |  | |  |  |
| 8 |  |  |  |  | |  |  |
| 9 |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
|  |  |  |  |  | |  |  |
| **填表人姓名** | |  | **填表日期** | | 年 月 日 | | |

# 十四、外来人员管理制度

## 第一章总则

为加强外来人员的管理，避免外来人员管理不善导致的风险，特制定此条例。

## 第二章适用范围

第一条      外部人员通常是指软件开发商，硬件供应商，系统集成商，设备维护商，和服务提供商，实习生，临时工等非内部人员。外部人员在访问时可以分成物理访问和信息访问，具体如下：

（一）      物理访问，如对办公室、机房的物理访问；

（二）      信息访问，如对信息系统、主机、网络设备、数据库的访问。

第二条      对于实际访问的外部人员，按照访问的时间长短和访问的性质，可以分为临时来访的外部人员，和非临时来访的外部人员两种，具体如下：

（一）      临时来访的外部人员，指因业务洽谈、参观、交流、提供短期和不频繁的技术支持服务而临时来访的外部组织或个人。

（二）      非临时来访的外部人员，指因从事合作开发、参与项目工程、提供技术支持、售后服务、服务外包或顾问服务等，办公和工作的外部组织或个人。

第三条      对于这两种短期和长期的实际物理和信息访问，应规定不同的安全管理要求，负责接待的部门和接待人对外部人员来访的安全负责，并对访问机房等敏感区域持谨慎态度。具体管理要求应包括：

（一）      遵守XXX的各项信息安全标准和管理规定；

（二）      必须签署保密协议，必须签署安全承诺协议，或在合同中规定相关的内容；

（三）      对其维护目标的安全配置要求，必须符合相应的网络设备、主机、操作系统、数据库和通用应用程序等XXX的安全配置标准文档中相应规定；

（四）      申请访问权限时，必须阐明其申请理由、访问方式、要求权限、访问时间和地点等内容，XXX的安全管理人员需要核实其申请访问权限的必要性和访问方式，评估其可能带来的安全风险，尽可能采取一些措施来降低风险。在风险可接受的情况下，才批准其访问权限的申请，并尽可能不给超级用户权限。

## 第三章附则

外来人员登记表



# 十五、变更管理制度

## 第一章总则

第一条 为规范XXX重要信息系统变更管理流程，控制变更产生的影响，减少变更发生的问题，保障信息系统安全运行和使用，特制定本规定。

第二条 本规定适用于XXX重要信息系统，包括计算机、网络、存储备份、输入输出等设备，以及系统、应用软件。

## 第二章变更定义

第一条 变更是指对系统/平台需求的增补或修改，所做增补或修改可能会影响生产环境的稳定性。变更区域包括但不限于硬件、系统软件(OS)、应用软件、网络、环境(冷却、供热等等)以及服务文件(如服务等级协议)。变更又分为计划型变更和应急变更。

第二条 影响系统安全状态的变更如：

1. 新的版本或修订；
2. 作业系统执行状态的变化；
3. 作业系统调度变更；
4. 网络设备软件安装补丁、更新。
5. 增/减软件或补丁；
6. 软件修改或增强；
7. 操作系统升级；
8. 增加/移动/变更相关信息系统使用单位、部门硬件配置，包括磁盘、磁带、CPU等；
9. 硬件和网络设备。

第三条 对于有计划的变更申请需要进行审批。变更前应预留一定的时间通知变更有关各方。通知时限取决于变更的严重程度。

第四条 应急变更是为了改正生产环境下的某一个重要问题而必须立即实施的变更。应急变更也需要进行审批，但在紧急情况下可免去通知时间和正常的变更程序要求。

## 第三章职责分工

第一条 XXX信息中心负责XXX的变更管理，主要职责为：

1. 审核变更申请的准确性；
2. 确认变更申请的记录信息的完整性；
3. 确保执行计划和变更失败倒回程序的质量；
4. 对变更申请予以批复；
5. 监督变更申请的执行情况；
6. 确保相关信息系统使用单位、部门根据变化情况修订有关文件和记录。

第二条 信息系统使用单位、部门的职责：

1. 根据实际运行情况，提出变更申请并在获得批准后执行变更；
2. 监督变更期间生产系统/平台的正常服务情况；
3. 确保倒回程序的实施足以恢复正常服务；
4. 根据情况的变化修订有关的文件和记录。

## 第四章 系统变更流程

第一条 信息系统在运行过程中产生的变更（包括用途、功能、性能等变更）变更应由变更申请人填写《信息系统运行变更申请表》（附表1），经各有关业务单位、部门确认后，由信息中心审核并提出意见，主管领导签字审批。

第二条 信息系统的配置（包括软件、硬件、系统等配置参数）变更应由变更申请人填写《信息系统配置变更申请表》（附表2），经相关运行维护单位、部门确认后，由信息中心审核并提出意见，主管领导签字审批。

第三条 信息中心领导对提交的变更申请审核审批后，应通知申请单位或部门，并对于批准的变更申请予以存档。

第四条 变更实施前，执行人应通知相关信息系统使用单位、部门的运行操作人员，以便变更进行时,监控变更期内系统和服务的运行情况。

如发现对服务有影响，维护人员应通知实施者，如果是因变更导致的影响，变更执行人应立即对问题进行调查，如问题严重，变更执行人应采取紧急恢复措施或倒回程序，和维护人员配合，务求恢复服务。

第五条 运行操作日志中应记录变更事件以备后查。

第六条 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。如果结果表明变更失败，变更执行人应采取回退措施将变更倒回到变更执行前的状态并进行测试，保证倒回成功。

第七条 完成变更步骤后，变更执行人在离开现场前要通知各信息系统使用单位、部门维护管理人员，进行验收程序。负责程序移植的人员需要进行移植情况的检查，留下书面的检查报告并签字确认。

第八条 属于信息资产配置变更范围内的，信息资产的维护单位、部门应根据《XXXXXX重要信息系统 资产安全管理规定》要求和变更情况，重新维护相应的信息资产信息和配置信息。

第九条 信息系统变更过程中应注意：

1. 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；
2. 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；
3. 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；
4. 应考虑新的技术和措施可能存在的安全风险。

第十条 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。

## 系统变更方案

## 新增服务器

第一条 适用范围：服务器进入XXX机房。

第二条 申请单位、部门填写变更申请单，并交申请、使用单位、部门和信息中心领导签字。

第三条 信息中心网络管理员为服务器分配机器名，以及IP地址（如果需要静态IP的话），确定机架位置。同时分配用于测试的临时IP地址。

第四条 申请单位、部门在机房安装服务器，部署、测试应用系统，系统运行部配合。测试时使用分配的临时IP。

第五条 部署、测试完成后，申请单位、部门向信息中心系统管理员移交服务器的管理员密码。

第六条 信息中心对服务器系统进行安全审核，清除不必要的系统帐号、停止不必要的服务、检查安全补丁安全装情况、防病毒程序安装、更新情况。按照运行部服务器补丁策略配置该服务器的补丁更新选项。

第七条 根据申请单位、部门备份需求，安装备份代理，更新备份策略。

第八条 检查应用系统的可能安全漏洞。

第九条 将服务器IP改为正式IP，将机器移到机架指定位置。

## 服务器迁移

第一条 适用范围：服务器移出XXX机房。

第二条 申请单位、部门填写变更申请，并交申请单位、部门领导签字。

第三条 关机拆除设备时，须通知信息中心，由信息中心专人拆除设备电源。

## 新建应用系统

第一条 申请单位、部门填写变更申请，经申请、使用单位、部门领导签字后，提交信息中心。

第二条 应提交以下文档作为变更申请单表的附件：

1. 上线说明书；
2. 系统说明书；
3. 系统测试报告；
4. 用户手册；
5. 运行手册。

第三条 信息中心系统管理员对文档进行审核后，进行变更风险评估，而后签字并交信息中心领导审批。

第四条 如果有必要，信息中心可进行应用安全评估。

第五条 信息中心系统管理员在工程或申请单位、部门相关人员指导和复核下进行新系统安装、部署工作。

## 应用软件变更

第一条 申请部门填写配置变更申请，经申请、使用单位、部门领导签字后，提交信息中心。

第二条 应提交以下文档作为变更申请表的附件：

1. 软件变更说明；
2. 安装说明。

第三条 信息中心系统管理员在开发或业务单位、部门相关人员指导和复核下进行程序变更的安装、部署工作。

## 第五章附 则

第一条 本规定由XXX信息安全领导小组办公室负责解释。

第二条 本规定自发布之日起执行。

**附表1**

**信息系统运行变更申请表**

|  |  |  |  |
| --- | --- | --- | --- |
| **申请单位、部门** |  | **申请人** |  |
| **申请日期** |  | **联系电话** |  |
| **变更类型** | □计划型变更 □应急变更 | **重要程度** | □高 □低 |
| **变更内容描述** |  | | |
| **申请更改时间** |  | **应用系统名称** |  |
| **实施期限/变更完成时间** |  | **特殊的变更指示** |  |
| **业务部门意见** | 签字:  日期： | | |
| **业务部门/用户/系统/平台的影响** |  | | |
| **变更前的准备工作** |  | | |
| **变更执行步骤** |  | | |
| **保证变更成功的测试方法** |  | | |
| **变更失败时应采取的回退程序** |  | | |
| **信息中心意见** | 签字:  日期： | | |

**广州附表2**

**信息系统配置变更申请表**

|  |  |  |  |
| --- | --- | --- | --- |
| **申请部门、单位** |  | **申 请 人** |  |
| **申请日期** |  | **联系电话** |  |
| **变更类型** | □计划型变更 □应急变更 | **重要程度** | □高 □低 |
| **配置变更内容** |  | | |
| **配置变更原因** |  | | |
| **配置变更方案** |  | | |
| **变更涉及的部门** |  | | |
| **通知部门**  **反馈意见** |  | | |
| **参与变更实施人员** |  | | |
| **实施人员** | 签字:  日期： | | |
| **信息中心意见** | 签字:  日期： | | |

# 十六、信息系统建设管理

## 第一章采购和安装

（一）软件的采购和安装

1．信息系统所使用的操作系统、应用软件、数据库、安全

软件、工具软件必须是正式版本，严禁使用测试版和盗版软件。

2．重要的操作系统和主要应用软件必须在安全管理员的监督之下进行安装。

（二）设备的采购和安装

1．设备符合系统选型要求并获得批准后，方可按相关政府采购流程进行购置。

2. 凡购回的设备均应在测试环境下经过连续72小时以上的单机运行测试和联机48小时的应用系统兼容性运行测试。

3. 通过上述测试后，设备才能进入试运行阶段。试运行时间的长短可根据需要自行确定。

4. 通过试运行的设备，才能投入系统，正式运行。

## 第二章软件开发管理（外包软件开发管理）

（一）应要求开发单位提供软件设计的相关文档和使用指南；

（二）在委托开发过程中，应加强开发过程中的安全管理和监控，重点考虑资质、许可证、代码所有权和知识产权；审核工作质量和访问权限，代码质量和安全功能达到合同要求。特殊情况应测试恶意代码和特洛伊木马。

（三）应要求软件开发商在所开发的信息系统内设计实现了安全控制措施，确保信息在系统中得到了正确处理。

（四）在开发过程中，应采取控制措施，减少信息泄露的可能性，重点考虑：规范开发过程中的通信行为，以减少第三方从这些行为中推断信息的可能性；在现有法律或法规允许的情况下，定期监视个人和系统的活动；监视计算机系统的资源使用；防止非授权的网络访问；对程序源代码的防护管理；

（五）要求软件开发商对程序源代码进行管理与控制。程序源代码应集中保存在代码库中，对代码库实施安全保护。保护措施主要包括：建立程序源代码和源程序库管理规范；对访问源程序库人员进行授权管制；程序列表应保存在安全的环境中；建立对源程序库所有访问的审核日志；维护和拷贝源程序库应受严格的限制；

（六）测试数据的管理。对于开发过程中涉及的测试数据。在测试数据选择过程中，应避免使用包含个人信息或其它敏感信息的运行数据库用于测试。其控制措施包括：运行信息每次被拷贝到测试系统时应有独立的授权；测试完成后，应立即从测试系统中清除运行信息或进行授权访问控制；记录运行信息的拷贝和使用日志；

（七）信息系统安全整体测试。组织信息系统使用部门在离线测试环境下对所开发信息系统进行安全测试。经过测试确认后，方可转入正式环境，并组织评估测试结果的安全符合性。

## 第三章工程实施

（一）指定或授权专门的部门或人员负责工程实施过程的管理，必要时可引入外部信息工程监理机构进行工程实施的监理。

（二）由实施方制定详细的工程实施方案经认可后控制实施过程，要求工程实施单位能按计划执行工程实施；

（三）由实施方制定工程实施方面的管理规范，明确说明实施过程的控制方法和人员行为准则，及时向本院提交相关表单文档。

## 第四章测试验收

（一）委托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，要求建设单位根据测试结果及时进行整改；

（二）在测试前应根据设计方案或合同要求等制订测试方案，在测试过程中应详细记录测试结果，并形成测试报告，测试通过后方可进行验收；

（三）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；

（四）指定或授权专门的部门或人员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；

（五）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。

## 第五章系统交付

（一）对系统交付的控制方法和人员行为准则进行书面规定；

（二）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。

（三）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和确认；

（四）对负责系统运行维护的技术人员进行相应的技能培训，以及对系统最终用户的操作进行相应的培训。

# 十七、系统运维管理规定

## 第一章 基本要求

## 总则

1. （办法目的）为建立健全医院信息系统运维体系，规范信息系统运维管理工作，保障信息系统安全、稳定运行，制定本规定。
2. （管理对象）本规定适用于医院运维管理涉及的软硬件基础设施和业务应用系统，包括但不限于机房、监控室、网络通讯、硬件设备、虚拟化云平台、操作系统、数据库、应用系统等。
3. （管理目标）信息系统运维管理应当遵守国家技术监管要求和技术标准，符合医院管理的各项规章制度，不断提高运维管理的制度化和规范化，保障医院信息系统的安全稳定运行。
4. (管理责任)在医院的统一协调下，各部门按照职责分工承担相关信息系统的运维管理责任，相互协同开展工作。
5. （约束范围）医院所有部门、正式员工和外包人员应当在开展信息系统运维工作时遵守本规定。

## 组织架构及岗位职责

1. 医院信息系统运维管理组织机构包括医院领导，以及运营部、产品部、运维部、研发部等技术部门。
2. 医院领导负责各部门之间的总体协调，全面指导、督促信息系统运维工作的开展。
3. 医院信息系统基础设施的运维工作包括机房、监控室、网络通讯、硬件设备、虚拟化云平台等的日常运维、监测监控、应急处置，及运维值班工作。基础设施运维管理由运维部负责。
4. 医院各业务系统的运维工作包括操作系统、数据库等系统软件及应用软件的日常运维、业务监控及应急处置。业务系统的运维管理由各业务部门负责。
5. 基础设施运维应配备网络管理员、系统管理员、安全管理员、机房管理员、值班专员等岗位，负责基础设施的运维管理工作，并设置主备岗。
6. 业务系统运维应配备系统管理员、数据库管理员、应用管理员、安全管理员等岗位，负责业务系统的运维管理工作，并设置主备岗。
7. 关键岗位进行分离，兼岗时满足岗位相互制约的要求。
8. 安全管理员督促解决在检查、测评、评估中发现的风险隐患。
9. 运维部负责机房运维，指定机房管理负责人，并配备机房运维人员，对机房的出入、服务器的开机或关机等工作进行管理。
10. 运维部指定运维值班负责人。运维值班负责人负责日常操作的部署、检查、风险控制、业务衔接等工作。运维值班负责人有备岗，主备岗不得同时离岗。
11. 机房管理员及值班人员负责控制、鉴别和记录设备和人员的进出情况，记录进出人员、进出时间、工作内容，并留存记录至少90天。
12. 运维部负责对网络进行管理，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。
13. 运维部负责等级测评的管理。
14. 运维部负责管理系统定级的相关材料，并控制这些材料的使用。
15. 研发部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。
16. 各业务部门负责管理事件的记录、分级、分派、处理、监控和结束整个流程。
17. 各业务部门应明确文档管理的责任人。
18. 各业务部门应明确数据管理责任人，负责数据收集、使用、备份、检查等策略的制定和执行工作。
19. 各业务部门应明确设备和软件管理责任人。
20. 各业务部门应明确责任人，负责统一保管、安全存放管理员口令，不得泄漏。
21. 各业务部门应对关键和敏感岗位进行重点管理，重要操作应当实行双人操作复核制度。

## 管理规程和技术规范

1. 运维管理规定覆盖运维工作各个环节，包括体系化的运维管理制度和操作流程。运维管理制度应包括但不限于：机房管理、值班管理、日常操作、监控分析、网络管理、系统管理、数据库管理、应用系统运维、数据和介质管理、权限与口令管理、事件与问题管理、交付与测试管理、变更管理、配置管理、监控室管理等流程。
2. 运维管理规定由运维部负责制定，经总办会审议后发布。
3. 医院建立统一的运维管理平台，通过信息化手段对事件管理、问题管理、变更管理等流程进行集中管理。

## 软硬件设备管理

1. 运维部对医院信息系统的硬件设备进行管理，各业务部门对各自信息系统相关的软件进行管理。设备和软件的出入库、维修（升级）、报废等工作应按照医院相关管理制度执行。
2. 运维部应及时更新信息系统相关的硬件设备管理清单，记录项目主要包括设备名称、设备编号、设备主要参数、设备序列号、设备保修期、设备上线年份、设备位置、设备用途和设备使用责任人等内容，并保留设备启用、转移、维修、报废等过程的记录。
3. 各业务部门应及时更新信息系统相关的软件清单，主要包括软件名称、软件编号、软件版本，授权和许可情况、软件序列号、软件状态、软件维护期、软件安装设备、用途和使用责任人等内容，并保留软件启用、转移、升级、报废等过程的记录。
4. 运维部应使用统一的设备标签对设备进行标识，标识应放在设备明显位置。
5. 运维部评估设备的使用年限，并对设备进行更新。各业务部门评估软件的使用年限，并对软件进行升级。

## 运维工作督促和检查

1. 运维部组织对医院各业务部门运维制度的执行情况和运维工作开展情况定期进行检查，以督促运维工作持续改进。
2. 检查范围至少包括对运维管理制度和操作流程的合理性和完整性进行评估，对运维管理制度和操作流程的执行情况进行评估，对文档、配置、数据的有效性进行评估，对整体安全状况进行评估等。
3. 各业务部门应对检查的结果采取纠正性和预防性的措施

## 第二章 运行保障

## 机房管理

1. 机房是支持各信息系统正常运行的基础设施，运维部负责建立机房管理制度，保障机房内设备稳定运行，构建可靠的IT运行环境。
2. 机房管理应涵盖物理环境管理、供电管理、设备管理、出入管理等内容。
3. 物理环境管理应包括温湿度、消防、防雷、防水、卫生及环境美观等内容。
4. 供电管理应包括UPS使用及维护管理、负载监控、电器使用等内容。
5. 设备管理应包括设备的上线、变更、下线、施工检修及日常操作等内容。
6. 出入管理应包括门禁、监控、人员进出登记等内容。

## 值班管理

1. 值班管理是信息系统正常运行的重要环节，应配备合格的技术值班人员，建立并完善值班管理制度及流程，规范日常监控及运维操作，以减少日常运维管理中的风险，及时发现系统运行安全隐患并对事件进行处理，避免系统事故给信息系统带来的影响。
2. 医院实行7\*24小时值班制，设置运维值班电话，并保持畅通。
3. 为保障值班工作的规范性，应制定相关的制度或管理细则，明确值班岗位设置、职责，值班工作内容、值班班次安排、值班要求及值班过程中的注意事项。
4. 值班工作应明确具体的值班人员和分工，值班工作至少涵盖日常操作、监控管理、机房管理、事件处理、问题处理以及应急处置等工作。
5. 值班人员应采用授权账号进行值班操作和监控，授予满足值班、监控工作最低的操作权限，并对授权账号的操作内容进行审计，以确保值班操作的准确性，避免人为操作失误造成的运行事故。
6. 为保证运维记录信息的有效性、完整性，应进行值班文档收集、整理、保管工作，值班文档保存期为一年。

## 日常操作

1. 日常操作是信息系统系统运行的基本环节，各业务部门应加强日常操作的管理，使日常操作标准化、规范化，提高系统运维质量，有效保障系统的运行安全。
2. 日常操作根据周期可分为每日、每周、每月等例行操作及非例行的特殊操作、临时操作,根据内容可分为机房基础设施、网络设备、主机、业务系统的健康检查、日常监控等。
3. 各业务部门应制定信息系统的日常操作规程，规程的内容应涵盖日常操作的具体工作内容，明确工作内容的对象、时间、步骤、指令、操作、复核等要点，并根据业务变化或系统变更进行及时修订。
4. 日常操作的相关表单内容，应如实填写操作、复核情况并进行签字确认。为进行有效的评估、统计以及审计、稽核，相关操作表单应由各业务部门管理员进行收集整理，并且进行妥善保管，保存时间为一年。
5. 运维部应对信息系统相关的各种设备（包括备份和冗余设备）、线路等指定专门人员定期进行维护管理；每季度至少进行一次维护管理。
6. 运维部应对终端计算机、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，按操作规程实现关键设备（包括备份和冗余设备）的启动/停止、加电/断电等操作。
7. 各业务部门应制定操作手册。操作手册的内容至少包括信息系统日常运行操作的各个环节，针对各个操作环节制定操作规程。

## 监控分析

1. 各业务部门应建立完善的监控分析体系，有效地监控系统各部件运行状态及容量、性能，提高系统突发事件的预警预报能力，及时掌握系统的运行情况，对发现的隐患、异常进行有效处理，避免或降低系统运行故障，确保业务连续性及服务质量。
2. 运维部负责对医院信息系统基础设施进行监控，各业务部门负责对各自业务系统进行监控。
3. 监控系统的覆盖范围应满足信息系统日常运维管理的需要，监控范围覆盖机房环境、网络设备及通信线路、运维主机、与业务相关的应用系统等对象，并实现多种报警方式，以便及时有效的通知相关运维人员。在部署自动化监控系统的同时，为避免其失效造成的疏漏，还需要采用人工巡检作为辅助手段。
4. 为避免监控系统部署不当对信息系统产生影响，需要根据不同的监控对象设定不同的监测频率，通过定期评估确定监控系统的阈值，使监控系统在有效运行的同时，不至于对信息系统产生不良影响。
5. 各业务部门需要有效管理和保存系统产生的日志信息，并定期进行分析、评估，及时发现系统运行过程中的隐患，减少系统运行事故的发生。

## 网络管理

1. 网络管理应涵盖安全管理、安全审计、访问控制、结构安全、身份鉴别、网络运维等部分。
2. 安全管理包括：
3. 能够检查内部网络用户采用双网卡跨接外部网络，或采用电话拨号、ADSL拨号、手机、无线上网卡等无线拨号方式连接其他外部网络。
4. 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。
5. 定期检查安全隔离情况，确保各安全域之间有效隔离。
6. 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。
7. 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提供报警。
8. 在网络边界处对恶意代码进行检测和清除。
9. 维护恶意代码库的升级和检测系统的更新。
10. 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。
11. 每季度至少进行一次漏洞扫描，对漏洞风险持续跟踪，在经过充分的验证测试后对必要的漏洞开展修补工作。
12. 实施漏洞扫描或漏洞修补前，对可能的风险进行评估和充分准备,如选择恰当时间，并做好数据备份和回退方案。
13. 在漏洞扫描或漏洞修补后进行验证测试，以保证网络系统的正常运行。
14. 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。
15. 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。
16. 合理设置安全域，绘制网络拓扑图，并保持更新。
17. 综合运用防火墙、入侵检测等安全设备，保护网络与系统；正确设置安全设备的接口参数和过滤规则。
18. 定期检查防病毒网关和邮件防病毒网关的恶意代码库的升级情况并进行记录，对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。
19. 安全审计包括：
20. 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。
21. 审计记录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。
22. 能够根据网络系统中的网络设备运行状况、网络流量、用户行为等日志记录进行分析，并生成审计报表。
23. 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。
24. 定期检查网络设备的用户、口令及权限设置的正确性。
25. 定期对系统容量进行检查和评估，形成评估报告。
26. 访问控制包括：
27. 网络边界部署访问控制设备并启用访问控制功能。
28. 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。
29. 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。
30. 限制具有拨号访问权限的用户数量。原则上不应通过互联网对重要信息系统进行远程维护和管理。
31. 在会话处于非活跃一定时间或会话结束后终止网络连接。
32. 限制网络最大流量数及网络连接数。
33. 重要网段采取技术手段防止地址欺骗。
34. 制定网络访问控制策略，合理设置网络隔离设施上的访问控制列表，关闭与业务无关的端口；编制文档并保持更新；访问控制策略的变更应履行审批手续。
35. 系统管理员、安全管理员、安全审计员等设备特权用户的权限应分离。
36. 采取限制IP登录等手段，控制对主机、主干网络设备、安全设备等的访问。
37. 结构安全包括：
38. 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。
39. 保证网络各个部分的带宽满足业务高峰期需要。
40. 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；业务终端和业务服务器应放置在不同的子网内，并建立安全的访问路径。
41. 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。
42. 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。
43. 重要网段与其他网段之间采取可靠的技术隔离手段。
44. 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。
45. 重要线路至少具有一条以上的备份线路。
46. 身份鉴别包括：
47. 删除默认用户或修改默认用户的口令，根据管理需要开设用户，不得使用缺省口令、空口令、弱口令。
48. 对网络设备的管理员登录地址进行限制。
49. 网络设备用户的标识应唯一。
50. 口令符合以下条件：数字、字母、符号混排，无规律的方式。
51. 管理员用户口令的长度至少为12位。
52. 管理员用户口令至少每季度更换1次，更新的口令至少5次内不能重复。
53. 如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。
54. 具有登录失败处理功能，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。
55. 当对网络设备进行远程管理时，采取必要措施防止鉴别信息在网络传输过程中被窃听。
56. 通过本地控制台管理主要网络设备时，采用一种或一种以上身份鉴别技术。
57. 以远程方式登录主要网络设备，采用两种或两种以上组合的鉴别技术进行身份鉴别。
58. 禁止通过互联网对防火墙、网络设备、服务器进行远程管理和维护，特殊紧急情况下采取限制登录IP、数字证书或动态口令认证、全程监控等措施，在操作完成后应及时关闭，并对维护过程进行监控并留存记录。
59. 网络运维包括：
60. 绘制与当前运行情况相符的网络拓扑结构图；绘制完整的网络拓扑结构图，有相应的网络配置表，包含设备IP地址等主要信息，与当前运行情况相符，并及时更新。
61. 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。
62. 持续跟踪厂商提供的网络设备的软件升级更新情况，在经过充分的测试评估后对必要的补丁进行更新，并在更新前对现有的重要文件进行备份。
63. 保证所有与外部系统的连接均得到授权和批准。
64. 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；在配置变更前、变更后分别对网络设备的配置文件进行备份。
65. 配置、调优网络系统的参数。
66. 禁止在业务时段对网络设备、安全设备、系统设备进行更换或变更配置。
67. 计算机网络跳线整齐干净，跳线标识清晰。
68. 对网络信息点进行管理，编制信息点使用表，并及时维护和更新，确保与实际情况一致。
69. 保持网络设备的可用性，及时维修、更换故障设备。
70. 定期对整个网络连接进行检查，确保所有交换机端口处于受控状态。

## 系统管理

1. 各业务部门应建立系统管理制度，对系统的运行维护进行规范。
2. 系统管理应包括：
3. 应保持系统的可用性，及时维修、更换故障设备和更新软件；
4. 应负责操作系统的参数配置、调优，编制文档并保持更新；
5. 应定期对系统容量进行检查和评估，形成评估报告；
6. 应负责管理系统和应用程序服务进程，并关闭与业务无关的服务；
7. 应定期检查操作系统的用户、口令及权限设置的正确性。
8. 操作系统管理员口令应符合以下条件：数字、字母、符号混排，无规律的方式。
9. 操作系统管理员口令的长度不少于12位。
10. 操作系统管理员口令至少每季度更换1次，更新的口令至少5次内不能重复。
11. 如果受限于操作系统，使得管理员口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。
12. 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。
13. 当对服务器进行远程管理时，采取必要措施，防止鉴别信息在网络传输过程中被窃听。
14. 为操作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。
15. 通过本地控制台管理主机设备时，采用一种或一种以上身份鉴别技术。
16. 以远程方式登录主机设备，采用两种或两种以上组合的鉴别技术进行身份鉴别。
17. 启用访问控制功能，依据安全策略控制用户对资源的访问。
18. 实现操作系统和数据库系统特权用户的权限分离。
19. 严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令。a)系统无法修改访问权限的特殊默认账户，可不修改访问权限；b)系统无法重命名的特殊默认账户，可不重命名。
20. 及时删除多余的、过期的账户，避免共享账户的存在。
21. 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。
22. 服务器主机的审计内容应包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。
23. 服务器主机的审计记录包括事件的日期、时间、类型、主体标识、客体标识和结果等。
24. 保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录至少保存6个月。
25. 服务器主机的审计范围覆盖到服务器和重要客户端上的每个操作系统用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。
26. 能够根据记录数据进行分析，并生成审计报表。
27. 保护审计进程，避免受到未预期的中断。
28. 操作系统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。持续跟踪厂商提供的系统升级更新情况，在经过充分的测试评估后对必要的系统补丁进行及时更新。
29. 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；针对重要服务器的入侵行为检测通过网络级或主机级入侵检测系统等方式实现。
30. 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。如不能正常恢复，应停止有关服务，并提供报警。
31. 对所有服务器和终端设备安装防木马、病毒等防恶意代码软件，定期进行全面检查，并及时更新防恶意代码软件版本和恶意代码库。a)原则上所有主机应安装防恶意代码软件，系统不支持该要求的除外；b)未安装防恶意代码软件的主机，应采取有效措施进行恶意代码防范。
32. 支持防恶意代码软件的统一管理。
33. 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。
34. 提高所有用户的防病毒意识，告知及时升级防病毒软件，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。
35. 定期检查主机防病毒产品的恶意代码库的升级情况并进行记录，对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。
36. 定期对服务器进行全面病毒扫描，但不得在业务时段内进行。
37. 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。
38. 根据安全策略设置登录终端的操作超时锁定。
39. 限制单个用户对系统资源的最大或最小使用限度。
40. 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。
41. 重要服务器的CPU利用率、内存、磁盘存储空间等指标超过预先规定的阈值后实时进行报警。
42. 对系统资源的使用进行预测，以确保充足的处理速度和存储容量，管理人员应随时注意系统资源的使用情况，包括处理器、存储设备和输出设备。

## 数据库管理

1. 各业务部门应根据业务需求建立数据库管理制度，对数据库的运行维护进行规范。
2. 口令应符合以下条件：数字、字母、符号混排，无规律的方式。
3. 口令的长度至少为12位。
4. 口令至少每季度更换1次，更新的口令至少5次内不能重复。
5. 如果设备口令长度不支持12位或其他复杂度要求，口令应使用所支持的最长长度并适当缩小更换周期；也可以使用动态密码卡等一次性口令认证方式。
6. 为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。
7. 审计内容至少包括：用户的添加和删除、审计功能的启动和关闭、审计策略的调整、权限变更、系统资源的异常使用、重要的系统操作（如用户登录、退出）等。
8. 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。
9. 保护审计记录，避免受到未预期的删除、修改或覆盖等。审计记录至少保存6个月。
10. 审计范围覆盖到服务器和重要客户端上的每个数据库用户；应在保证系统运行安全和效率的前提下，启用系统审计或采用第三方安全审计产品实现审计要求。
11. 能够根据记录数据进行分析，并生成审计报表。
12. 保护审计进程，避免受到未预期的中断。
13. 保持数据库的可用性，及时维护、更新软件。
14. 对数据库的参数进行配置、调优，编制文档并保持更新。
15. 定期对数据库容量进行检查和评估，形成评估报告。
16. 管理数据库、表、索引、存储过程，数据库的升级、优化、扩容、迁移。
17. 定期检查数据库的用户、口令及权限设置的正确性。

## 应用系统运维

1. 各业务部门应建立应用系统运维制度，对应用系统的运行维护进行规范。
2. 应用系统运维操作流程应包括但不限于日常操作、事件处理、问题处理、系统变更、应急处置等流程。
3. 业务系统的操作规程至少包括操作的对象、时间、步骤、指令、操作要点、复核要点、操作人、复核人等基本要素。
4. 严格按照操作手册执行运维操作，对业务系统的操作过程进行记录留痕，记录的保存时间不少于一年。
5. 特殊操作、临时操作应经批准后方可双岗执行。操作过程进行记录留痕，记录的保存时间是否不少于一年。
6. 依据业务、信息系统的变化，对操作手册及规程进行及时修订，经审批通过后遵照执行。
7. 采取人工值守和自动化工具相结合的方式，对业务系统进行 24 小时监控。业务高峰时段应指定人员对业务系统进行监控，其他时段如无法做到人工监控，应开启自动监控系统和自动报警系统。
8. 正确设置自动化监控工具的预警阈值，并定期进行检查和评估。
9. 业务相关的应用系统监控指标包括进程的活动状态、日志信息、中央处理器使用率、内存利用率、并发线程数量、并发处理量、关键业务指标等。
10. 针对不同系统设置合理的监测频度。
11. 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。
12. 应对应用系统的参数配置、调优，编制文档并保持更新。

## 数据与介质管理

1. 各业务部门应按照国家和监管部门的有关要求，根据数据的重要性及其对系统运行的影响，制定数据备份及验证策略，明确备份范围、备份方式、备份频度、存放地点、存放时限、有效性验证方式。
2. 运维部根据备份策略，对信息系统相关数据进行备份。各业务部门负责对备份数据的恢复验证。
3. 运维部应将应制定相关的数据备份与介质管理规定，对数据的备份、存放、保护等进行规范管理。
4. 运维部应对介质的转储、送修、销毁及存储环境进行管理。
5. 确保介质存放在介质库或档案室等安全的环境中，并实行存储环境专人管理，实现对各类介质和备份数据的控制和保护。
6. 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。
7. 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。
8. 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，涉密信息的存储介质不得自行销毁，应按国家相关规定另行处理。
9. 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。
10. 在线数据未经授权不得访问、复制。
11. 对数据的修改应通过审批，双岗操作并记录操作日志。
12. 离线数据不得更改。
13. 离线数据的调阅、复制、传输、查询，应按照拟定的流程办理审批手续，并进行登记。
14. 备份数据带离存储环境时应采取必要的安全措施。
15. 在线数据和离线数据用于非生产环境时，应进行脱敏处理；用于模拟测试时如无法进行脱敏处理，测试环境应采取与生产环境相当的安全措施。
16. 离线备份介质应在本地机房、同城安全可靠存放。
17. 涉及敏感信息的介质送修时应由专人全程陪同，并保证修复过程可控。
18. 对外送设备的维修进行严格管理，防止数据泄露。
19. 对拟下线和拟报废设备的存储介质中的全部信息进行清除或销毁。对正式下线设备和软件由运维部统一管理、保存或处置，并保留相应记录。设备和软件报废符合资产管理规定。
20. 对执行程序、源代码及相关文档应采取严密措施妥善、安全保管。

## 事件与问题管理

1. 事件管理的目的是在尽可能小地影响业务的情况下使系统尽快恢复到服务级别协议所定义的服务级别，保障业务正常进行，提高用户满意度。
2. 医院应建立事件管理流程，对信息系统运维事件的处理进行规范。
3. 事件处理流程一般包括事件报告、记录、分级、分派、处理、监控和结束等阶段。事件处理中的角色一般包括事件管理小组、事件报告人、事件管理人、事件处理人等。
4. 运维部与各业务部门应协同配合，共同处置信息系统故障。运维部负责排查基础设施故障，业务部门负责排查业务系统故障。由各业务部门负责事件报告。
5. 记录运维过程中发生的所有事件，根据事件的影响程度和影响范围评估事件处理优先级及时处理。
6. 对所有事件响应、处理、结束等过程进行跟踪、督促及检查。
7. 定期回顾、分析事件处理记录，完成事件分析报告。
8. 对安全检查情况进行评估，形成评估报告。
9. 问题是指导致一起或多起事故的潜在的、不易发现的原因。对于重复发生的事件、原因未明的事件、重大事件纳入问题管理，通过建立问题管理机制，对问题的处理进行跟踪、管理，最终使系统运维中的问题得以解决。
10. 问题处理流程一般包括问题的识别与提交、分类、分析、处理、解决和结束等阶段。问题处理中的角色一般包括问题管理小组、问题提交人、问题处理人、问题管理人等。各业务部门都可以承担问题提交人的角色。
11. 医院信息系统基础设施问题由运维部负责提交、分析、处理、关闭；各业务系统问题由各部门负责提交、分析、处理、跟踪、关闭事件。
12. 应将运维过程中重复发生的事件、重大事件纳入问题管理。
13. 应将监控、分析、自查、检查、测评、评估和事件处理中发现的问题进行汇总，并纳入问题库。
14. 各业务部门应组织对问题进行分析、提出解决方案、通过变更管理审批后部署实施，并将解决过程归纳整理并纳入问题库。

## 第三章 系统维护

## 交付与测试

1. 医院应建立交付流程，对建成的信息系统交付运行维护的活动进行规范。
2. 各业务部门应制定交付工作清单，作为双方交付依据，清单包括信息系统相关的软件、硬件、技术文档、管理手册、使用手册、培训材料、相关工具、协议和合同等。
3. 各业务部门应对运维人员和所涉及的相关各方进行培训和说明，包括交付事项的目的、范围、背景、测试要求、上线实施要求、验收要求、运维要求等。
4. 各业务部门应制定交付实施计划，划定交付双方的职责，交付的步骤，并对交付过程留存记录。
5. 各业务部门应建立系统测试流程，对系统上线前进行的模拟环境测试和生产环境测试进行规范。
6. 各业务部门应为系统测试配备必要的人员和设备资源，需要时应协调关联单位配合测试。
7. 各业务部门应根据系统上线要求制定测试方案，确定采用的测试方法和测试流程。测试方案及测试用例应覆盖功能、性能、容量、安全性、稳定性等方面。测试完成后应对测试结果进行分析评估，并给出测试报告。
8. 模拟环境测试的要求如下：
9. 应建立独立的模拟环境。模拟环境应在逻辑架构上和生产环境一致。模拟环境应与生产环境进行分离，不得对生产环境进行干扰；
10. 应根据测试方案的设计，合理配置测试所需的设备，识别设备不同可能带来的测试结果正确性风险；
11. 可根据需要，要求业务部门组织业务人员参与测试；
12. 模拟环境使用的密码应与生产系统严格区分，系统管理员宜由不同的人员担任。
13. 生产环境测试的要求如下：
14. 测试前应备份当前系统的数据和配置；
15. 应提前发布系统测试公告；
16. 应由各业务部门生产系统运维人员在生产环境下组织完成；
17. 应根据需要，要求业务部门组织业务人员参与测试；
18. 根据测试的结果设计系统升级过程及应急预案；
19. 如果测试内容涉及其他相关系统，应协调其他系统用户参与测试；
20. 测试后应恢复生产环境并验证恢复的有效性；

## 系统变更

1. 医院应建立系统变更流程，对信息系统的变更活动进行规范。
2. 各业务部门应确认系统中要发生的变更，并制定相应的变更方案；重要系统变更前制定详细的变更方案、失败恢复方案、专项应急预案。
3. 各业务部门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。
4. 各业务部门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。
5. 各业务部门应建立系统变更流程，对信息系统的变更活动进行规范。
6. 各业务部门应明确系统变更中的角色，至少包括：申请人、审批人、实施人、复核人。
7. 变更申请人提交正式的变更申请，申请中应有明确的变更方案，内容至少包括：目标、对象、时间、人员、紧急程度、操作步骤、测试方案、实施方案、风险防控措施、应急预案、回退方案等。
8. 变更审批人应在充分评估变更的技术风险和业务风险的基础上进行审批，审批记录应留痕并满足审计需要。
9. 变更审批人应确定变更实施时间窗口，除紧急变更外，不得在业务时段进行变更实施。
10. 各业务部门应按照测试方案，组织变更前后的测试，测试后提交测试记录或报告。
11. 变更实施人应按照变更实施方案进行变更，并及时更新配置库。
12. 变更复核人应对变更记录和变更结果进行评估，评估内容是否至少包括变更目标的达成情况、对生产环境的影响、配置库更新情况。
13. 各业务部门应定期检查变更控制的申报和审批程序的执行情况，评估系统现有状况与文档记录的一致性。
14. 重大的系统变更升级应组织用户进行严格的联网测试，制定专项的应急预案和回退方案。
15. 各业务部门应在开展重大信息系统项目建设、迁移或改造时，应事前向安全管理小组进行报告，并定期报告项目进展情况。

## 配置管理

1. 运维部应建立配置库，并负责对信息系统的服务器、存储、网络等配置进行管理，各业务部门负责对操作系统、应用软件、数据库等配置进行管理。
2. 各业务部门应合理设置配置库中配置项的属性，要求如下：
3. 配置项属性至少包括编号、名称、描述、维护责任人、运行状态、关联关系等；
4. 配置项编号应唯一；
5. 配置项的添加、修改、替换、删除应有变更记录；
6. 应保存配置项历史记录，确保与事件管理、问题管理、变更管理等流程记录的关联性。
7. 运维部应定期对配置库进行备份。
8. 各业务部门应及时检查并定期审计配置库，对发现的不一致情况及时纠正，并留存记录。

## 第四章 监控室管理

## 出入管理

1. 运维部应建立监控室出入管理流程，对设备和人员出入进行严格管理。
2. 运维部应指定人员负责控制、鉴别和记录设备和人员的进出情况，非运维部人员进出监控室应进行登记。
3. 外来人员进入监控室应经过申请和审批流程，并限制和监控其活动范围，并有医院人员陪同。

## 终端与介质管理

1. 监控室内必须使用运维部提供的指定的终端设备进行操作。
2. 所有监控室内终端设备与介质的出入和报废应由运维部运维人员负责登记和妥善处理，防止相关信息的对外泄漏，保障信息的安全。
3. 未经运维部批准，禁止将笔记本电脑、相关存储设备及未经检查的软件介质等进入生产环境。接入生产环境的设备及介质必须确保无病毒感染。

## 堡垒机与授权管理

1. 堡垒机由运维部统一管理；
2. 堡垒机权限应经过审批后开通。堡垒机系统账户的建立，需经申请部门及运维部负责人审批，堡垒机访问业务系统的授权，需由业务系统所在部门相关负责人审批。
3. 堡垒机口令应符合以下条件：数字、字母、符号混排，无规律的方式，口令的长度不少于12位。
4. 堡垒机的访问日志由运维部统一保存。