**医院信息安全规划**

一、医院信息安全问题分析

目前医院各项业务发展迅速，信息系统陆续上线运行，但是信息安全规划和实施相对滞后。部分安全技术防护措施缺失，恶意代码防范、安全异常监控、日志分析审计等能力相对薄弱，不能及时发现和定位信息安全事件，信息系统安全风险控制能力有待加强。2017年医院漏洞扫描、跳板机被控、勒索病毒等暴露出了医院当前突出的信息安全问题：

1、基础架构方面，网络区域之间隔离策略有待加强和检查，网络接入认证手段有限；未建立定期补丁更新机制，操作系统补丁、数据库关键补丁欠缺，windows服务器未统一安装防病毒软件等。

2、应用系统方面，安全漏洞频发，开发需求及设计评审环节主要关注业务层面的系统实现，缺乏安全管控要求；缺乏上线前后服务、进程、端口、配置信息等系统安全运行状态跟踪比对。

3、用户管理方面，弱口令和口令重用风险突出，部分系统均被发现存在弱口令现象，同一系统多台服务器使用相同密码的现象屡次出现；用户身份与账号权限管理手段单一，用户权限合理性有待验证。

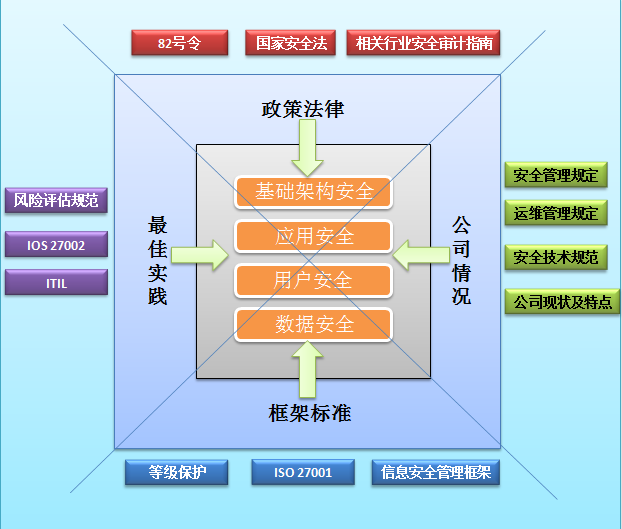
4、数据方面，缺乏敏感信息分类分级管理，数据保护措施不足，无法对敏感数据信息查询、访问、备份等操作进行安全审计，缺乏针对移动介质和内部的管控措施，目前渲染数据无冗余备份。

5、安全管理方面，日志分析、安全监控等基础安全措施不到位，缺乏安全基线管控手段，对信息系统安全状态缺乏掌握，信息系统风险评估、等级保护尚未开展。

二、医院信息安全规划目标

信息安全体系建设是一个持续演进、不断发展过程，围绕国家安全法、风险评估、等级保护及其它行业审计指南等监管要求，结合医院信息化建设规划，参考国内外信息安全标准、实践指南等，对医院信息安全建设进行总体规划，根据安全建设方向的轻重缓急进行分步实施。

通过技术和管理两大方面的安全措施，实现信息系统生命周期安全管理，实现基础架构、应用系统的安全、高可靠，实现敏感数据访问、用户权限认证的安全控制，最终达到IT管理与安全管理的良性互动。



图一 信息安全规划目标

三、医院信息安全规划原则

为了保证医院信息系统安全管理的一致性，在对信息系统进行规划设计、开发建设、运行维护和变更废弃的安全性考虑时，应充分遵循以下安全原则：

1、符合性原则

符合国家的法规要求的前提下，参照国内外标准构建符合自身需求的信息安全体系。保证安全建设的先进性、完整性、全面性。

2、整体性原则

“木桶的最大容积取决于最短的一块木板”，安全问题往往发生在系统最薄弱的环节。安全机制设计的首要目的是防止最常发生和最主要的问题，根本目的是提高整个系统的"安全最低点"。

3、可靠性原则

信息安全建设一般采用业界成熟的最佳实践，不能过分求全求新，防止不必要的失误。运用阶段性的设计和实施方法保证信息安全建设能够有控制的进行。

4、可发展性原则

在考虑解决现有信息安全问题的同时，还需要考虑信息化的发展和变化，为将来的扩充和调整留有充分的余地。要根据信息化建设的变化不断调整安全措施，适应新的网络环境，满足新的信息安全需求。

5、整合共享原则

就是要充分整合、利用、发挥现存网络基础、业务系统和信息资源，促进互联互通，资源共享。

四、信息安全技术设施规划

根据信息安全规划目标，从安全运营、基础架构、应用系统、数据、用户等方面增加安全技术措施，形成完善的安全监控、检测、防护、响应和分析能力。技术设施规划如下图所示，绿色标记为已经具备，红色标记为需要建设。



图二 信息安全技术设施规划

1、安全运营管理

（1）安全配置基线系统

安全配置基线管理是医院内部信息安全管理的重要组成部分，是医院开展安全巡检和风险评估等工作的前提和基础。建设安全配置基线系统，在系统上线部署、运行维护阶段推行基础配置合规检查、弱口令专项核查、防火墙策略专项核查、补丁安装专项核查等，满足信息系统的最基本的安全要求，实现信息系统内网络设备、操作系统、数据库等安全配置的自动化检测。

（2）安全扫描检测系统

部署多套专业、异构的安全扫描、检测工具，提升漏洞扫描的准确性和全面性，及时发现医院内网信息系统安全漏洞，支撑内网安全巡检工作开展。

（3）安全监控系统

建立安全监控系统，全面覆盖互联网系统、内网系统安全监控，增强事件发现能力。互联网监控通过对医院对外开放的信息系统资产的IP、端口、应用模块、敏感文件等进行可用性、安全性监控，及时发现外部威胁；内网安全监控综合应用异常流量分析、入侵行为分析、病毒木马检测、文件沙箱检测等，对多源异构数据进行关联识别，及时发现内网的异常行为、入侵攻击和可疑文件，提高安全事件发现能力。

（4）安全日志分析系统

建设日志分析系统，汇总采集医院信息系统内网络设备、操作系统、中间件、数据库、安全设备及应用系统等的日志信息，通过格式化日志信息，抽取关键字段，利用大数据关联分析技术，发现外部非法入侵及内部异常操作等安全事件。

（5）安全智能中心

建立安全智能中心，以大数据的收集、处理与分析技术为驱动，通过引入外部威胁情报，结合安全监控、日志分析等系统，对网络环境、主机应用及威胁情报数据进行长时间、大范围的关联分析，实现从基于规则匹配向数据建模、机器学习智能化的转变，从短时间状态监控向长周期趋势变化及动态基线转变，从单一事件监控向整体态势感知转变，从依靠自身安全能力向威胁情报共享、风险预测的转变，形成医院的统一安全感知防护体系，最大限度的保护信息资产安全。

2、基础架构安全

通过完善网络安全基础架构，规范网络接入安全管理，提高网络、系统层对病毒、漏洞、木马、拒绝服务攻击等的安全防御水平，提高网络安全事件分析能力。具体措施包括：

（1）网络安全隔离措施

划分医院网络安全区域，部署防火墙等安全隔离设备，完善业务系统相关端口管理，严格限制访问控制策略，实现网络安全区域之间的有效隔离。引入数据交换隔离措施，满足不同区域之间数据安全传输和安全控制需要。

（2）内容安全防护系统

统一部署防恶意代码、防病毒软件，加强医院服务器主机、办公终端的病毒及恶意代码防范能力。密切关注防垃圾邮件、勒索软件邮件等防护技术进步，及时增强医院邮件系统的安全防护能力。

（3）漏洞补丁跟踪管理系统

建设漏洞补丁跟踪管理系统，采集医院信息系统内部资产信息，识别操作系统、数据库等主要软件类型，及时督促信息系统更新重要补丁。对医院办公终端补丁进行统一下发。

（4）WAF、DDOS防护系统

利用WAF、DDOS防护系统对互联网DDOS、WEB攻击进行实时检测、阻断，妥善应对可能遭受的拒绝服务攻击、入侵攻击、恶意扫描等攻击行为，有效降低互联网信息系统安全风险。

3、应用系统安全

在应用开发生命周期中，加强开发安全管理、安全编码和安全测试，切实提高应用系统安全能力。具体措施包括：

（1）安全设计导入

系统建设需求设计阶段，引入安全需求分析，定义系统安全架构，建立系统安全控制模块，降低系统被入侵的可能性。

（2）安全编码机制

系统开发阶段，引入安全编码机制，定义安全编码函数，保障开发过程安全。

（3）应用安全测试

系统验收测试阶段，依据医院应用安全测试规范，对上线系统执行应用安全测试，及时发现安全漏洞，保障系统上线后安全稳定运行。

（4）移动APP安全加固

建设移动APP应用安全加固系统，保障医院应用系统安卓和IOS平台移动APP应用的安全。通过移动应用渠道安全监测，及时发现互联网上针对医院移动APP应用的篡改、盗版等攻击。

4、用户权限安全

规范化的、全方位的管理IT用户的授权和访问行为，统一管理“用户-岗位-角色-账号”的关联关系；对用户的敏感业务操作和敏感数据访问进行集中审计和监督。具体措施包括：

（1）引入用户安全集中管理系统，对医院各部门的服务器、网络设备、安全设备以及信息系统进行统一管控，并实现对用户帐号、系统帐号、用户权限、用户身份认证、用户行为审计的统一管理。

（2）探索采用双因素强身份认证、单点登录、系统帐号口令接管等技术机制，解决帐号共享、帐号口令管理困难、密码重用等用户安全管理难题。

5、文档数据安全

对敏感数据的访问授权、保存和交换进行细粒度控制和跟踪审计。逐步建立集中式的文档管理系统和文档密级管理。具体措施包括：

（1）敏感数据防泄密

逐步细化对医院敏感数据的访问授权、保存和交换的管理和跟踪审计，探索建立敏感数据防泄密系统，对医院的敏感资料、业务数据等机密数据做出标记，实时隔离和阻挡非授权的传播行为。

（2）数据文档权限管理系统

逐步加强医院数据、文档权限控制，探索建立文档权限管理系统，严格控制数据访问、文档阅读、修改、外发权限，实现敏感文档的密级管理、授权管理，防止文档信息外泄。

五、信息安全管理措施规划

安全管理措施是信息系统安全管理的形式化、具体化的接口，是信息安全得以实现的重要保证。梳理安全工作流程，将安全工作体现在信息系统生命周期中的规划、设计、开发、测试、运行、下线等各个阶段，以贯彻落实国家安全法、风险评估、等级保护、ISO 27001要求，保证安全工作的最终落地。

1、等级保护工作

完成重要信息系统的等级保护备案、定级、测评等工作。每年对等级保护二级及以上的信息系统进行测评工作。

2、安全风险评估

开展医院信息系统的风险评估工作，建立风险评估工作流程，调研风险评估工具，每年至少完成1-2次风险评估工作。

3、内部安全巡检

开展医院内部安全巡检工作，建立内网安全巡检工作流程，丰富巡检工具手段，防范安全巡检操作风险。每季度对医院内网所有生产、测试信息系统进行安全扫描，对医院网络区域间隔离情况进行检查，对系统帐号的权限和口令进行检查。每年对医院所有生产环境信息系统进行一次渗透测试和安全配置检查。

4、系统安全检测

加强系统上线安全检测工作，建立规范的系统安全检测标准，规范检测工作流程，完善检测手段，提高检测效率。

5、ISO 27001体系建设

调研ISO27001信息安全管理体系在国内相关企业执行情况，依据ISO27001信息安全管理体系标准要求，调研、评估医院信息资产存在的安全风险，优化医院信息安全整体规划，建设完整的信息安全管理体系，待条件成熟时申请ISO27001认证。

6、安全意识及技能培训

人员素质是保证安全的根本，需要通过不断的培训来提高。建立安全培训体系，根据内部人员的责任分工，工作重点不同而分层面，有重点地进行安全培训工作。

（1）普及型安全培训

对于非安全管理相关人员的安全培训可采用安全讲座、定期分发相关安全知识宣传资料等方式进行。内容包括安全意识培训、安全知识普及培训、医院信息安全管理规定等规章制度培训。

（2）专业型安全培训

专业型安全培训是针对医院相关部门骨干技术人员的培训，在对普及型培训的基础上，进行更深入层面的安全技术、安全管理的培训，可通过搭建模拟的测试环境、现场演示攻防等，开展信息安全技术基础、攻防技术培训、信息安全产品培训、安全事件紧急响应等培训内容。