
深圳市人口健康信息化建设项目

信息安全体系建设需求

深圳市医学信息中心

(2018年9月)

一、信息安全体系建设参考依据

(一) 国家、部委政策文件

《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)

《国家信息化领导小组关于加强信息安全保障工作的意见》(中办发[2003]27号)

《关于信息安全等级保护工作的实施意见》(公通字[2004]66号)

《信息安全等级保护管理办法》(公通字[2007]43号)

《“十三五”全国人口健康信息化发展规划》(国卫规划发(2017)6号)

《基于健康档案的区域卫生信息平台建设技术方案(试行)》, 卫生部, 2009

《基于健康档案的区域卫生信息平台建设指南(试行)》, 卫生部, 2009

卫生部《基于电子病历的医院信息平台建设技术解决方案》

卫生部 基于健康档案的区域卫生信息平台建设指南（试行）

（二）国家信息安全标准及等级保护政策文件

《GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求》

《GB/T 22240-2008 信息系统安全等级保护定级指南》

《GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求》

《GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求》

《GB/T 20984-2007 信息安全技术 信息安全风险评估规范》

《GB/T 20009-2005 信息安全技术 操作系统安全评估准则》

《GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求》

《GB/T 20270-2006 信息安全技术 网络基础安全技术要求》

《GB/T 20272-2006 信息安全技术 操作系统安全技术要求》

《GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求》

《GB/T 18336-2008 信息技术 安全技术 信息技术安全性评估准则》

《GA/T 671-2006 信息安全技术 服务器技术要求》

《GA/T 672-2006 信息安全技术 终端计算机系统安全等级技术

要求》

ISO27000 系列

ISO20000 系列

以及其他相关标准

(三) 电子政务安全标准规范

《国家电子政务外网网络与信息安全管理暂行办法》

《政务外网信息安全标准化工作规范》

《政务外网安全监测体系技术规范与实施指南》

《政务外网安全等级保护基本要求》

《政务外网安全等级保护实施指南》

《政务外网云计算安全等级保护设计基本要求》

《政务外网安全基线基本要求》

《政务外网 IPSec VPN 安全接入技术要求与实施指南》

《政务外网安全接入平台技术规范》

《(专线) 接入政务外网的局域网安全技术规范》

《政务外网统一互联网出入口安全保障技术规范》

《政务外网安全接入平台实施指南》

《政务外网安全管理系统功能技术要求及接口规范》

《政务外网安全审计技术要求（网络行为与运维管理）》

《政务外网审计系统技术要求》

《政务外网业务应用安全基本要求》

《政务外网跨网数据安全交换技术要求与实施指南》

《政务外网网络与信息安全事件分类及通报管理规范》

《政务外网总体应急预案规范》

《政务外网网络攻击、木马病毒等应急预案规范》

《政务外网数据备份恢复管理规范》

《政务外网运维故障处理安全规范》

二、安全域的划分

按照深圳市人口健康信息化建设项目中各应用分类，结合其安全需求，可以将平台划分为卫生专网、互联网两个接入网络：卫生专网和互联网，卫生专网有重要的业务系统与数据，要求做好安全防护和数据防窃取，这两张网要求实现物理隔离。通过前置机和隔离网闸做好必要的交互与物理隔离，实现卫生专网与互联网的物理独立性。

（一）根据网络结构，进行大的安全域的划分

卫生专网内部需要做好安全域的规划与隔离，按照逻辑区域建议将整体网络划分成出口边界、核心交换区、DMZ区、内网业务系统安全域等。安全域之间做好逻辑隔离（VLAN逻辑隔离）、安全防护与访问控制部署的基础安全防护策略。

（二）根据业务类型，进一步划分安全子域

按照“分区分域、纵深防护”的思路，以业务的维度进行安全子域的划分。根据《深圳市人口健康信息化建设项目初步设计方案》，项目内建设的主要应用系统包括：

1、基于卫生专网的业务系统类。

主要是公共卫生、计划生育、医疗服务、医疗保障、药品供应、行业管理等不同的业务区域内主要的生产系统。其中部分系统设计为等保二级，部分系统设计为等保三级。

2、基于互联网的业务系统类。

主要是面向公众的健康惠民信息服务、查询服务、信息公开、大数据服务等业务。应根据业务的重要性，进一步分为二级、三级的等保业务区域，并实施相关的安全策略。

3、市级人口健康信息平台类及基于平台的应用系统。

包括：数据采集与交换、基础平台系统、基于平台的业务协同应用系统、基于平台的综合管理应用系统等。

安全域划等级划分示意图如下：

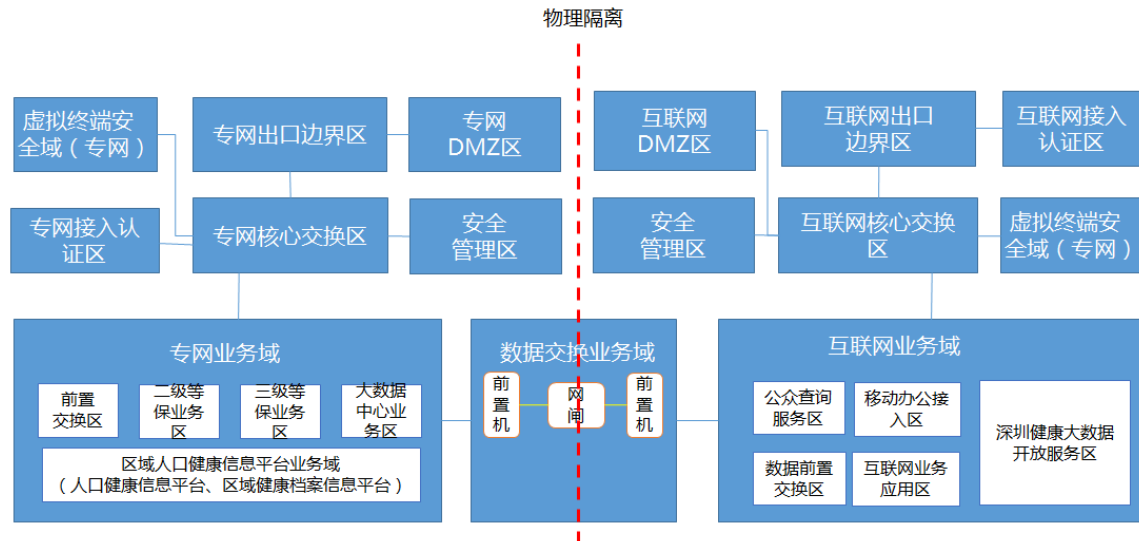


图1 安全域划等级划分示意图

三、信息安全设备需求情况*

按照《深圳市人口健康信息化建设项目初步设计方案》，本项目信息安全设备需求如下表所示：

序号	设备名称	明细内容
1	防火墙	
2	抗 DDOS 服务	
3	链路负载均衡	
4	IPS	
5	防病毒网关	
6	数据库审计	
7	WAF (含网页防篡改)	
8	集中运维安全管理系统	
9	网闸	
10	统一身份管理认证系统	<ul style="list-style-type: none"> ◇ 统一身份管理 ◇ 统一身份认证
11	网络安全态势感知	<ul style="list-style-type: none"> ◇ 网络安全态势感知设备 ◇ 网络入侵态势感知系统 ◇ 异常流量态势感知系统 ◇ 僵尸蠕虫态势感知系统 ◇ 系统漏洞态势感知系统 ◇ 网站安全态势系统
12	集中安全审计平台	
13	主机安全保护系统	
14	流量控制系统	
15	IDS	
16	漏洞扫描	
17	异常流量溯源系统	<ul style="list-style-type: none"> ◇ 异常流量溯源设备 ◇ IP 溯源系统 ◇ 流量溯源系统 ◇ 行为溯源系统 ◇ 地图溯源系统
18	信息安全态势感知系统	<ul style="list-style-type: none"> ◇ 信息安全态势感知设备 ◇ 信息安全态势感知系统
19	数据共享保护系统	<ul style="list-style-type: none"> ◇ 数据支撑平台数据交换与服务访问前置系统 ◇ 数据支撑平台跨网数据安全交换系统 ◇ 数据集成平台跨网数据交换集控系统

序号	设备名称	明细内容
		<ul style="list-style-type: none"> ◇ 数据集成平台跨网数据交换集中审计系统 ◇ 数据集成平台安全隔离与信息交换系统
20	异常流量检测	
21	前置机数据库防火墙软件	

*注：此表所列设备及说明仅做参考，并非最终采购需求。

深圳市医学信息中心