长宁区文化和旅游管理事务中心
信息安全等级保护咨询测评项目

建设单位：长宁区文化和旅游管理事务中心

编制时间：2023 年 10 月

目录

第 1 章 项目概况

1.1 项目名称

1.2 长宁区文化和旅游管理事务中心网络信息安全等级咨询测评项目

1.3 项目单位

长宁区文化和旅游管理事务中心

1.4 建设依据

1.4.1 政策依据

1. 深入贯彻习近平总书记关于网络强国的重要思想，落实《网络安全法》《数据安全法》《个人信息保护法》《密码法》《关键信息基础设施安全保护条例》《上海市数据条例》有关规定

2. 中共中央办公厅 国务院办公厅印发《“十四五”文化发展规划》;

3. 文化和旅游部《“十四五”文化和旅游发展规划》(文旅政法发〔2021〕40 号);

4. 文化和旅游部《“十四五”文化和旅游科技创新规划》(文旅科教发〔2021〕39 号);

5. 《推进上海生活数字化转型构建高品质数字生活行动方案(2021—2023 年)》;

6. 《长宁区全面推进城市数字化转型行动方案(2021-2023)》。

1.4.2 参考标准

（1）《信息安全技术个人信息安全规范》(GB 35273-2020);

（2）《信息安全技术信息技术产品供应方行为安全准则》(GB/T 32921-2016);

（3）《计算机软件开发规范》(GB8566-88);

（4）《计算机软件产品开发文件编制指南》(GB8567-88);

（5）《计算机软件质量保证计划规范》(GB/T12504-90);

（6）《计算机软件需求规格说明规范 GB/T9385-2008》;

（7）《计算机软件测试文档编制规范 GB/T9386-2008》;

（8）《计算机软件可靠性和可维护性管理 GB/T14394-2008》;

（9）《计算机软件测试规范 GB/T15532-2008》。

1.5 建设背景

“十四五”时期是我国在全面建成小康社会基础上开启全面建设社会主义现代化国家新征程的第一个五年，我国文化和旅游发展仍然处于重要战略机遇期，但机遇和挑战都有新的发展变化，满足人民日益增长的美好生活需要，需要顺应数字化、网络化、智能化发展趋势，以5G网络、人工智能、大数据、云计算、物联网、区块链等新一代信息技术为代表的新一轮科技革命和产业变革进一步深入发展，数字技术更

加全面融入社会交往和日常生活，以智能化、数字化为目标的数字经济快速增长，构筑智慧便捷、全民畅享的美好数字生活新图景，已经成为广大人民群众美好生活新期待的重要内容。

1.6 建设必要性

1.6.1 响应国家文化和旅游发展规划政策的需要

为进一步推进文化事业、文化产业和旅游业繁荣发展，根据《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》，2021年4月，文化和旅游部印发《“十四五”文化和旅游发展规划》发展积极健康的网络文化”。

1.6.2 服务于上海长宁区城市数字化转型的需要

通过排查了解掌握文旅局重要网站、平台、生产系统，数字资源的风险和防护状况，摸清网络和数据安全底数，达到以查“促建、促管、促防、促改”的目的，推动局机关与关联单位网络安全工作责任制全面落实，提升安全防护水平。真正做到数据赋能和关键支撑，打造具有示范效应的数字政务标杆场景。

1.6.3 强化网络信息安全监管的需要

2020年9月，文化和旅游部出台《通知》根据长宁文旅的实际情况和的需求提供安全策略和措施，保障系统内各单位网络的安全性，包括

Web 应用安全、网络与基础架构安全、业务安全。并且能够对网络安全事件进行快速反应，有效地减少由于安全问题引起的损失。

具体内容包括：

⑴ 网络信息安全管理：

⑵ 网络信息安全巡检：

⑶ 网络信息安全处置：

⑷ 网络信息安全分析：

⑸ 信息安全系统等级保护专业咨询测评

1.6.4 改造和预防信息数据安全监管应用场景的需要

在海量数据内容面前，单靠审核人员人工来把关越来越不现实：一方面，海量的信息数据带来的成本压力与日俱增。另一方面，人工的时效性无法满足目前各种实时在线数据的需求，国家有关部门的监管力度在不断加大，要求越来越严，利用网络信息安全设备处理、信息安全软件技术，专业信息安全技术团队技术支持等手段，解决多环境多场景下的技术障碍，提供各种信息全专业建议，大大改善了工作的时效性和效率，同时大幅降低了成本。

1.7 建设目标

1.7.1 助力整体网络信息安全提升

建立完善的网络信息安全机制的建立和各类制度，做好权限管理、明确责任人，做好网络信息安全预案和应急演练工作。

对长宁文旅信息化软硬件设备进行梳理，了解网络情况，绘制整网逻辑拓扑图。对已有安全措施和设备运行状态进行确认，开展定期巡查、漏扫和病毒查杀，杜绝隐患发生。

对发现网络信息安全问题及时处置、发生突发网络安全时间及时响应，配合做好系统设备安全策略加固、规则库更新、增加监控与防御手段，使网络、系统安全高效运行。

利用日志分析设备、安全设备策略分析、漏洞扫描结果分析、基线扫描结果分析、设备运行状况分析、业务数据流向分析，为健全网络安全管理手段做数据支撑。

对长宁文旅局在政务外网和互联网端的重要网站、平台、生产系统，下属事业单位的注册登记地确定。具体工作如下：

(一)局机关重要网站、平台、生产系统的数量、分布情况、主管单位、网络安全组织管理和运维保障情况，数据存储情况，个人信息和重要数据的安全保护及处理活动情况，信息安全技术防护情况等

(二)下属事业单位网站、平台、生产系统（自研软件系统）的主要功能、服务范围、信息安全等保情况。

1.7.2 健康有序发展

通过提升，最大限度降低信息安全隐患，保护国有数据合法权益，促进文旅局数字信息健康有序发展，更好地为人民群众多样化、多层次的精神文化需求提供优质服务。

1.8 网络信息安全运维整体规划

(一) 网络安全组织工作开展

开展网络信息安全工作、梳理的重要网站、平台、生产系统情况。

(二)重要网站、平台、生产系统确定情况

确定重要网站、平台、生产系统数量、分布、功能等情况。所涉及的个人信息和重要数据的处理活动情况。

(三)信息安全重点内容

一. 网络安全管理措施具体情况。按照《党委(党组)网络安全工作责任制实施办法》《上海市各级党委(党组)网络安全工作责任制实施细则》,明确了网络安全直接责任人;制订并落实了网络安全事件应急预案;外包系统按要求以合同协议等形式明确安全责任:对系统进行安全防护检测，并形成有法律效力的测评报告。

二. 网络安全防护技术措施。启用电子邮件系统双因子登陆认证，及时删除离职人员账户、严格审计邮件访问行为、关闭邮件自动转发功能;关闭或删除不必要的系统、网站、应用、服务、端口和链接; 是否存在重要漏洞未修复情况，是否存在弱口令、默认口令、通用口令和长期未更换的口令;系统开发者、运维者是否使用了开源代码管理平台，是否修改了默认配置并严格访问控制策略;对重要数据、重要功能进行备份等。

三. 个人信息和重要数据安全保护排查。规范数据采集渠道、采集流程和采集方式;采取加密保护措施，保证数据安全传输:明确数据资产的使用人和安全责任人:制定数据分类分级管理制度;配置访问控制管理和安全审计;明确各类数据销毁场景及销毁方式;关闭外联数据接口杜绝向境外提供重要数据或个人信息。

1.9 本项目建设目的

为全面推进长宁区数字化转型，聚焦文旅数字化需求，以满足局机关的网络信息安全环境，各个分支单位自研开发的软件系统，更好地满足区域内市民多样化、多层次的精神文化需求。

1.9.1 网络信息安全管理：

做好网络安全机制的建立和各类制度的健全，做好权限管理、明确责任人，做好网络安全预案和应急演练工作。降低工作人员监管成本，大幅提升工作人员工作效率。

1.9.2 网络信息安全检查：

通过对长宁文旅信息化软硬件设备进行梳理，了解网络情况，绘制整网逻辑拓扑图。对已有安全措施和设备运行状态进行确认，开展定期巡查、漏扫和病毒查杀，杜绝隐患发生。

1.9.3 网络信息安全处置能力：

通过专业网络信息安全技术团队在发现网络安全问题及时处置、发生突发网络安全时间及时响应，配合做好系统设备安全策略加固、规则库更新、增加监控与防御手段，使网络、系统安全高效运行。

1.9.4 网络信息安全分析

基于客户端上传，支持对敏感文件标签化管理；支持对上传格式支持 txt、doc、xls 等格式，利用日志分析设备、安全设备策略分析、漏洞扫描结果分析、扫描结果分析、设备运行状况分析、业务数据流向分析，健全网络信息安全管理手段做数据支撑。

1.9.5 信息安全等级咨询测评

长宁文旅新建或等保过期的信息化系统的网络安全等级保护咨询评测，共有伍个系统需要开展等保测评工作：

⑴ 长宁区图书馆智慧阅读系统（系统已上线等保已过期，软件有更新需重新进行系统信息安全评估）

⑵ 非遗中心智慧书房（系统已上线缺安全咨询与等保测评）

⑶ 演出市场内容智能监管系统（系统已上线缺安全咨询与等保测评）

⑷ 长宁区图书馆官方网站平台系统（系统已上线等保已过期）

⑸ 长宁区图书馆资源直通车系统（系统已上线等保已过期）

1.10 总投资估算

本项目总投资估算57.93万元，

第2章 项目现状

2.1 项目单位概况

上海市长宁区文化和旅游管理事务中心(上海市长宁区文物管理事务中心）承担长宁区文化和旅游市场管理、文物管理、资源开发和产业发展、以及文化和旅游公共服务宣传推广等工作。上海市长宁区文化和旅游管理事务中心（上海市长宁区文物管理事务中心）共有 6 个内设

机构，包括：办公室、市场管理部、文物管理部、资源开发和产业发展部、公共服务部、信息化工作部。

长宁区图书馆坐落在天山路356号(地铁2号线威宁路1号出口处)，是沪上最大的城区图书馆，约16000平方米建筑面积12个层面，设计藏书50余万册，1000余种中外报刊杂志，1200个阅览坐席，国际交流访问中心、新书展示区、读者休闲区、中外文报刊阅览区、展览展示区、图书借阅区、青少年图书 阅览区、参考资料阅览区、多媒体图书阅览区、特色馆藏阅览区、教育培训中心、多功能演讲厅，集图书、展览展示、教育培训为一体。

第3章 项目需求分析

3.1 业务需求分析

3.1.1 专业网络信息安全运维需求

长宁文旅的实际情况和的需求提供安全策略和措施，保障系统内各单位网络的安全性，包括Web应用安全、网络与基础架构安全、业务安全。并且能够对网络安全事件进行快速反应，有效地减少由于安全问题引起的损失。减少高风险信息产生，减轻工作人员实际工作量。

3.1.2 信息安全等级保护咨询测评需求

长宁文旅新建或等保过期的信息化系统的网络安全等级保护咨询评测费用。共有伍个系统需要开展等保测评工作：

⑴ 长宁区图书馆智慧阅读系统（复测评，需重新咨询评估）

⑵ 遗中心智慧书房（预评估等保三级）

⑶ 出市场内容智能监管系统（预评估等保三级）

⑷ 长宁区图书馆官方网站平台系统（复测评）

⑸ 长宁区图书馆资源直通车系统（复测评）

3.2 安全需求分析

3.2.1 整体安全需求

目前信息系统在运行环境、身份识别、网络安全、数据安全、应用系统安全以及信息安全综合管理方面均需加强安全防护能力，避免给整个信息系统带来严重安全威胁，尽可能的减少网络安全方面的隐患，保证网络的高性能、高稳定性及高可管理性。

平台需要严格遵照信息安全等级保护相关国家标准对信息系统进行分析整改并提供相应的等级保护安全服务。在开展信息安全等级保护安全建设整改工作中，按照国家有关规定和标准规范要求，坚持管理和技术并重的原则，将技术措施和管理措施有机结合，建立信息系统综合

防护体系，提高信息系统整体安全保护能力。依据《信息系统安全等级保护基本要求》，落实信息安全责任制，建立并落实各类安全管理制度，开展人员安全管理、系统建设管理和系统运维管理等工作，落实物理安全、网络安全、主机安全、应用安全和数据安全等安全保护技术措施。

信息安全等级保护咨询测评按照三级等保级安全保障措施进行建设实施。

3.2.2 访问控制需求

非法访问主要包括非法用户的非法访问、合法用户的非授权访问及假冒合法用户非法访问。非法用户的非法访问也就是黑客或间谍的攻击行为；合法用户的非授权访问是指合法用户在没有得到许可的情况下访问了他本不该访问的资源；假冒合法用户非法访问是指入侵者假冒合法用户的 IP 地址或用户名等对资源进行非法访问，这些非法访问都会对系统的安全性造成严重的损坏，因此，要采取一定的身份认证机制和访问控制手段，防范非法访问、入侵和攻击，严格控制只在合法用户才能访问合法资源。

3.2.3 传输加密需求

加密传输是网络安全重要手段之一。信息的泄漏很多都是在链路上被搭线窃取，数据也可能因为在链路上被截获、被篡改后传输给对方，

造成数据真实性、完整性得不到保证。如果利用加密设备对传输数据进行加密,使得在网上传的数据以密文传输。对数据传输过程中的完整性、真实性进行鉴别。可以保证数据的保密性、完整性及可靠性。因此，必需配备加密设备对数据进行传输加密。

3.2.4 防病毒系统需求

针对防病毒危害性极大并且传播极为迅速,必须配备从客户端到网关的整套防病毒措施，实现全网的病毒安全防护。

3.2.5 应用安全需求

随着互联网技术的迅猛发展,许多关键业务越来越多地基于WEB应用，为满足这种对外连接不可信任网络的业务安全需求，应专门在计算服务器池内，为业务应用设立专用服务器进行WEB应用部署，并在前端添加安全防护。

3.2.6 数据库安全需求

数据库安全是整个安全体系的重要组成部份,是信息安全保护的关键，数据库的安全需求主要有以下几方面：

（1）账号集中管理系统需求

账号集中管理系统，实现集中化帐号管理和身份验证，获得更高的控制能力和运行效率。实现整个帐户管理流程自动化，实现基于角色的

账户管理、策略执行、职能分工和管理权限委派等。可以对账号管理流程实现安全、可审核的内部控制。

（2）数据库安全审计系统需求

数据库安全审计系统是针对数据库的安全而提出的一种数据库操作审计产品，其基本思想是通过对网络数据的实时采集，以及对各种上层数据库通讯协议数据的实时分析和还原，对被监控网络中的数据库使用情况进行监控，对各种违规行为实时报告，甚至对某些特定的违规主机进行封锁，以帮助网络管理员对数据库资源进行有效的管理和维护。

3.3 其他需求分析

3.3.1 数据备份要求

提供自动备份功能，支持全系统每天实行增量备份，定期实行全量备份并且备份结果可恢复。

3.3.2 可扩展性要求

作为一个复杂的集中式应用系统，为多种类型的用户服务，技术实现时必须综合考虑系统的可靠性、高效性、安全性及业务发展的要求，也要适应和满足不同用户信息化发展的不同层次和水平，提供多样性的数据采集、接入和管理服务。

要充分考虑技术体系发展前景，适应未来发展的需要。在设计时充分考虑系统对其它设备和技术的兼容性，系统应该适应业务发展和变革的需要，适应新增设备的变化。

3.3.3 易操作性要求

针对系统易用性的具体要求：软件操作界面要清晰、简洁、便于操作和维护，尽量使用户能够不通过培训就可学会系统的使用。

3.3.4 异常处理要求

当系统出现致命异常，都要中止程序执行、回滚事务，应用程序自动记录异常前的正常数据，并以友好的方式提示用户，将错误信息写入日志，系统恢复后应可以查询或打开异常前的数据状态。

第 4 章 项目建设方案

等级保护 2.0 咨询，测评服务

长期密切关注并跟踪国家等级保护相关政策，协助使用方进行等级保护试点、重要信息系统定级、等级保护整改等多项工作，在等级保护工作实践中积累丰富经验。

等级保护 2.0 服务级别涵盖信息系统现状调研、定级备案、预测评、建设整改、等保测评及监督检查等各个环节，用户可根据自身实际情况选择具体服务，服务详情如下：

1.1. 现状调研

信息系统现状调研，可了解目标系统基本情况，详情如下：

信息安全管理制度调研，通过访谈了解安全管理制度建设情况。各项安全观制度覆盖范围，包括覆盖物理、网络、主机系统、数据、应用、建设和运维管理内容、安全相关人员、安全管理制度等基本情况。

信息安全技术调研，了解目标系统所涉及的物理机房、业务应用软件、关键数据类别、主机/存储设备、终端、网络互联设备、安全设备等情况。

1.2. 定级备案

协助用户单位，依据《信息系统安全等级保护定级指南》，确定信息系统安全保护等级。指导客户准备备案材料及备案支持。根据前期准备材料指导填写备案材料，协助客户向网安递送备案材料。

2.2.1. 辅助系统定级

依据《网络安全等级保护定级指南》所提出的 4 个定级要素，灵活运用指南中所提出的确定信息系统安全保护等级的步骤和方法，在信息系统业务安全性分析的基础上，提出等级建议，协助用户进行系统定级。

表-定级要素与安全保护等级的关系

受侵害客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	第一级	第二级	第二级
社会秩序、公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

2.2.2. 完成定级备案

协助用户完成系统安全等级备案工作：编制定级报告，填写备案表，三级以上系统协助用户完成备案资料的收集和整理，编制定级总结报告。

2.2.3. 上报定级备案材料

协助客户递交材料、领取备案证明等工作。

1.3. 等保预测评

根据系统情况调研的结果，针对互联网系统开展网络安全评估，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心等方面，对互联网信息系统内的物理机房、网络架构、网络设备、安全设备、服务器、应用系统等开展全面预测评并进行客观、准确分析。详情如下：

了解目标系统所涉及的物理机房、业务应用软件、关键数据类别、主机/存储设备、终端、网络互联设备、安全设备等情况。

2.3.1. 服务方式

等级保护咨询服务采用人员访谈、设备检测、实地查看相结合方式，分为现场服务和远程服务。

咨询顾问将根据授权咨询服务范围开展咨询服务。在充分考虑客户安全需求后，制定详细解决方案，并具体进行实施。

服务方式	人员访谈	设备检查	实地查看	具体实施
现场服务	顾问访谈	漏洞扫描上机 查看	物理机房 实地查看	安全整改、建设
非现场服	人工分析、方案设计	渗透测试	文档查阅	方案设计、制度

务				建设

2.3.2. 预测评内容

预测评服务范围包括安全通用安全、云计算安全、移动互联网安全、物联网安全、工业控制系统安全等领域。以安全通用安全（三级）为例，预测评内容如下，

2.3.2.1. 安全物理环境

序号	测评项	预测评方式	问题描述
1	物理位置选择	实地查看、文档查阅	
2	物理访问控制	实地查看、文档查阅	
3	防盗窃和防破坏	实地查看、文档查阅	
4	防雷击	实地查看、文档查阅	
5	防火	实地查看、文档查阅	
6	防水和防潮	实地查看、文档查阅	
7	防静电	实地查看、文档查阅	
8	温湿度控制	实地查看、文档查阅	
9	电力供应	实地查看、文档查阅	
10	电磁防护	实地查看、文档查阅	

2.3.2.2. 安全通信网络

序号	测评项	预测评方式	问题描述
1	网络架构	人员访谈、设备检查、文档查阅	

2	通信传输	人员访谈、设备检查、文档查阅	
3	可信验证	人员访谈	

2.3.2.3. 安全区域边界

序号	测评项	预测评方式	问题描述
1	边界防护	人员访谈、设备检查、文档查阅	
2	访问控制	人员访谈、设备检查、文档查阅	
3	入侵防范	人员访谈、设备检查、文档查阅	
4	恶意代码和垃圾邮件防范	人员访谈、设备检查、文档查阅	
5	安全审计	人员访谈、设备检查、文档查阅	
6	可信验证	人员访谈	

2.3.2.4. 安全计算环境

序号	测评项	预测评方式	问题描述
1	身份鉴别	人员访谈、设备检查、文档查阅	

2	访问控制	人员访谈、设备检查、文档查阅	
3	安全审计	人员访谈、设备检查、文档查阅	
4	入侵防范	人员访谈、设备检查、文档查阅	
5	恶意代码防范	人员访谈、设备检查、文档查阅	
6	可信验证	人员访谈	
7	数据完整性	人员访谈、设备检查、文档查阅	
8	数据保密性	人员访谈、设备检查、文档查阅	
9	数据备份恢复	人员访谈、设备检查、文档查阅	
10	剩余信息保护	人员访谈、设备检查、文档查阅	
11	个人信息保护	人员访谈、设备检查、文档查阅	

2.3.2.5. 安全管理中心

序号	测评项	预测评方式	问题描述
1	系统管理	人员访谈、文档查阅	
2	审计管理	人员访谈、文档查阅	

3	安全管理	人员访谈、文档查阅	
4	集中管控	人员访谈、文档查阅	

2.3.2.6. 安全管理制度

序号	测评项	预测评方式	问题描述
1	安全策略	人员访谈、文档查阅	
2	管理制度	人员访谈、文档查阅	
3	制定和发布	人员访谈、文档查阅	
4	评审和修订	人员访谈、文档查阅	

2.3.2.7. 安全管理机构

序号	测评项	预测评方式	问题描述
1	岗位设置	人员访谈、文档查阅	
2	人员配备	人员访谈、文档查阅	
3	授权和审批	人员访谈、文档查阅	
4	沟通和合作	人员访谈、文档查阅	
5	审核和检查	人员访谈、文档查阅	

2.3.2.8. 安全管理人员

序号	测评项	预测评方式	问题描述
1	人员录用	人员访谈、文档查阅	
2	人员离岗	人员访谈、文档查阅	
3	安全意识教育和培训	人员访谈、文档查阅	
4	外部人员访问管理	人员访谈、文档查阅	

2.3.2.9. 安全建设管理

序号	测评项	预测评方式	问题描述
1	定级和备案	人员访谈、文档查阅	
2	安全方案设计	人员访谈、文档查阅	
3	产品采购和使用	人员访谈、文档查阅	
4	自行软件开发	人员访谈、文档查阅	
5	外包软件开发	人员访谈、文档查阅	
6	工程实施	人员访谈、文档查阅	
7	测试验收	人员访谈、文档查阅	
8	系统交付	人员访谈、文档查阅	
9	等级测评	人员访谈、文档查阅	
10	服务供应商选择	人员访谈、文档查阅	

2.3.2.10. 安全运维管理

序号	测评项	预测评方式	问题描述
1	环境管理	人员访谈、文档查阅	
2	资产管理	人员访谈、文档查阅	
3	介质管理	人员访谈、文档查阅	
4	设备维护管理	人员访谈、文档查阅	
5	漏洞和风险管理	人员访谈、文档查阅	
6	网络和系统安全管理	人员访谈、文档查阅	
7	恶意代码防范管理	人员访谈、文档查阅	
8	配置管理	人员访谈、文档查阅	
9	密码管理	人员访谈、文档查阅	
10	变更管理	人员访谈、文档查阅	
11	备份与恢复管理	人员访谈、文档查阅	
12	安全事件处置	人员访谈、文档查阅	
13	应急预案管理	人员访谈、文档查阅	
14	外包运维管理	人员访谈、文档查阅	

2.4. 建设整改

提供符合等保相关要求的安全产品和服务，指导客户进行定级相关系统和组件的安全加固，并建立安全管理制度体系。

2.5.1. 技术整改

帮助用户建立的信息安全体系是符合客户实际情况，经济、高效、落地性强，基于等级保护 2.0 的信息安全建设方案。用户可根据自身情况选择相应搭配，包括基础组合、开源组合、云组合等。

基础组合示例

序号	设备类型	成效
1	下一代防火墙	满足认证管理、授权管理、安全区域边界建设管理、网页防篡改要求。
2	杀毒软件	满足恶意代码防范要求，防止来自外部病毒、恶意代码入侵等风险 满足安全计算环境要求、恶意代码防范要求
3	日志审计系统	通过日志审计，提前发现问题并解决，避免安全事件发生 满足审计管理要求、安全管理中心要求

2.5.2. 管理整改

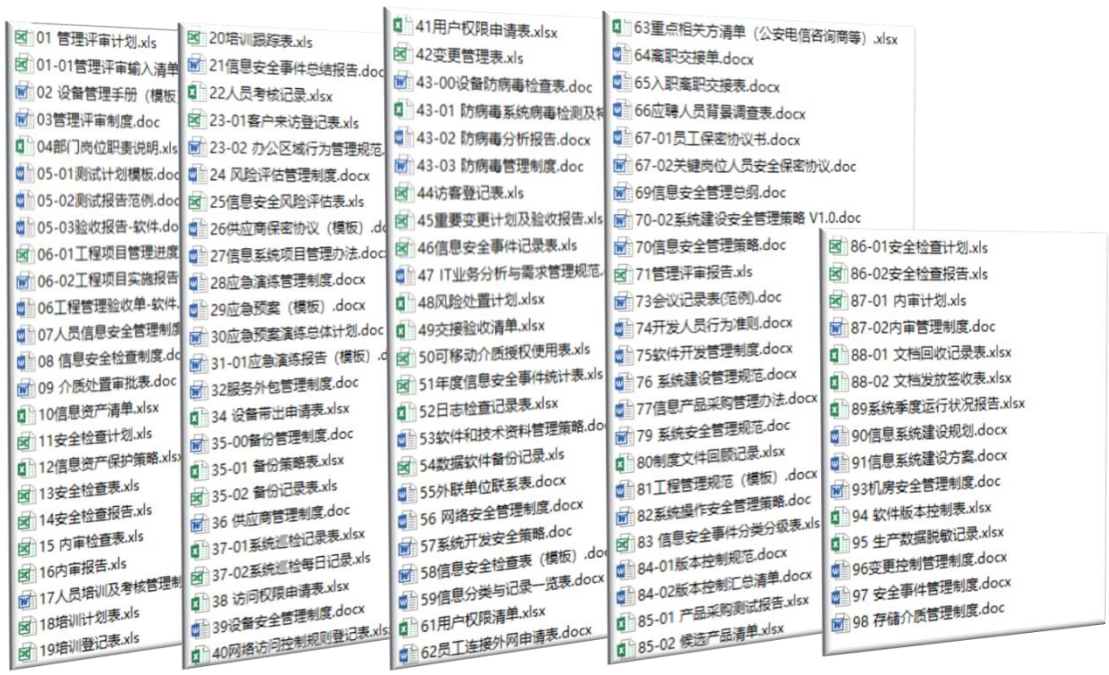
基于等级保护基本要求,根据行业最佳实践，建立符合企业特色的信息安全体系。基本包括如下内容：

一、建立安全管理体系

二、建立安全技术体系

三、建立安全运营体系

样例如下：



2.5.3. 其他特殊说明

按网安最新要求，需提交《大数据安全测评补充项》， 根据客户实际情况，协助客户完成该项表单的填写并提交。

2.5.4. 周期性服务

为满足单位网络安全建设及监管要求， 可持续提供周期性服务，包括渗透测试、漏洞扫描等。

2.5. 等保测评

与多家测评机构深度合作，提高测评通过率。

测评过程中，现场全程陪同客户进行测评，确保测评通过。

2.6. 监督检查

定期（至少每年一次）对信息系统安全状况、安全保护制度、安全保护措施落地情况进行评估。协助用户单位通过系统复测。

为用户提供定期的等保复测安全服务，为企业系统全生命周期运行保驾护航。

2.7. 等保服务交付

项目交付

√《等保 2.0 系统备案表》

√《等保 2.0 系统备案补充表》

√《等保 2.0 系统定级报告》

√《等保 2.0 系统信息调研表》

√《等保 2.0 等保预测评报告》

√《等保 2.0 管理制度补充及相应记录模板》

√《大数据安全测评补充项》

测评机构交付

√《等级保护测评报告》

网安交付

√《等级保护备案证明》

◆ 备注：以上所有项目交付清单，由华臻统一交付于客户，无需客户额外花费过多时间及经理沟通对接。

3. 项目管理

3.1. 人员安排

商务人员1位：负责项目中的商务洽谈，时间把控，沟通协调，保证需求精准对接，项目的顺利实施。

技术支持人员2位：等保项目技术主管+技术实施，专项负责对项目过程中出现的技术问题进行解答并指导客户完成测评内容，为客户排疑解惑。

项目经理1位：专享项目管理，负责项目中内部相关事项的沟通协调，合理调配各项资源，内部把控，保证项目的顺利实施。

3.2. 项目流程

序号	项目内容	工作内容	时间
1、现场调研			
1.1	项目前期沟通	对所有系统进行梳理，确定需要被测系统。	2DAY
1.2	项目人员确定	根据被测系统确认测评过程中参与配合人员。	1DAY
1.3	系统基本情况调研	对被测系统的基本情况进行调研，分析其中拓扑结构。	2DAY

1.4	项目启动会	前期准备完毕，项目正式启动。	1DAY
2、定级备案			
2.1	系统定级	根据前期准备材料指导填写备案材料。	3DAY
2.2	系统备案	协助向网安递交备案材料。	20DAY
3、 项目预测评			
3.1	安全物理环境咨询	咨询被测系统的物理安全，如物理位置的选择、防盗窃和防破坏、防雷击、防火等。	5DAY
3.2	安全通信网络咨询	咨询被测系统的网络架构、通信传输、可信验证。	3DAY
3.3	安全计算环境咨询	咨询被测系统的身份鉴别、安全审计、入侵防范恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护。	
3.4	安全区域边界咨询	咨询被测系统的边界防护、访问控制、入侵防范、恶意代码防范、可信验证。	
3.5	安全管理中心咨询	咨询被测系统的系统管理、审计管理、安全管理、集中管控。	
3.6	安全管理制度	对安全管理制度的制定、发布、修订、评审等流	

	咨询	程的各项制度进行逐项确认。	
3.7	安全管理机构咨询	对安全管理机构设置、机构制度、机构流程进行逐项确认。	
3.8	人员安全管理咨询	对被测系统的技术和管理人员的录用、离职、考核等各项制度进行确认。	
3.9	系统建设管理咨询	对被测系统的系统建设、方案设计、采购流程、开发流程、测试验收流程的各项规章制度进行确认。	
3.10	系统运维管理咨询	对被测系统的系统运维管理制度，包括网络安全、设备介质管理、系统安全等方面的规章制度进行逐项确认。	
4、建设整改			
4.1	差距分析	根据单元咨询的结果给出整改建议。	15DAY
4.2	整改沟通	协助对系统问题项进行整改。	15DAY
5、等保测评			
5.1	整体测评	测评机构依据等保标准进行测评。	7DAY
5.2	测评整改	测评中如测出特殊必需整改项需进行整改。	20DAY

5.3	复测	对特殊必须整改项进行复测。	3DAY
6、等保证明领取阶段			
6.1	测评报告提交	测评机构依据测评结果编制测评报告提交网安。	3DAY
6.2	网安审批	网安审批通过后通知测评机构，测评机构联系被测单位在测评报告上盖章，再提交至网安。	20DAY
6.3	领取证明	被测单位到网安领取等保证书。	1DAY

4.1 现场服务支持规范

测评服务人员要做到耐心、细心、热心的服务。工作要做到事事有记录、事事有反馈、重大问题及时汇报。严格遵守工作作息时间，严格按照服务工作流程操作。

(1) 现场支持工程师应着装整洁、言行礼貌大方，技术专业，操作熟练、严谨、规范；现场支持时必须遵守用户单位的相关规章制度。

(2) 现场支持工程师在进行现场支持工作时必须在保证数据和系统安全的前提下开展工作。

(3) 现场支持时出现暂时无法解决的故障或其他新的故障时，应告

知用户并及时上报负责人，寻找其他解决途径。

(4) 故障解决后，现场支持工程师要详细记录问题的发生时间、地点、提出人和问题描述，并形成书面文档，必要时应向用户介绍故障出现的原因及预防方法和解决技巧。

4.2 问题记录规范

根据使用人员提出问题的类别，将问题分为咨询类问题和系统缺陷类问题二类：咨询类问题是指通过服务热线或现场解疑等方式能够当场解决用户提出的问题，具有问题解答直接、快速和实时的特点，该问题到现场支持人员处即可中止，对于该类问题的记录可使用咨询类问题记录模版进行记录。系统缺陷类问题是指使用人员提出的问题涉及到系统相应环节的确认修改，需要经过逐级提交、诊断、确认、处理和回复等环节，处理解决需要各外包服务项目组的分析确认，问题有解决方案后，将解决方案反馈给用户。具体提交流程如下：

(1) 问题提交。应用信息系统的用户发现属于系统缺陷类的问题时，填写系统缺陷类问题提交单，提交服务支持人员。

(2) 问题分析。服务支持接到用户提交的问题单，要组织相应人员对问题单中描述的问题进行分析研判，确定问题的类型(技术问题、业务问题或者操作问题)。属于技术问题，提交服务技术人员对存在的问题提出具体的处理意见和建议；属于业务问题，

提交服务业务人员进行处理；属于操作问题，可安排相关人员对问题提出人进行解释，并将系统缺陷类问题提交单转为系统咨询类问题提交单。

(3) 问题确认、解决。服务的技术人员和业务人员收到系统缺陷类问题提交单后，对提交的问题进行归类汇总和分析、确认。可以解决的，明确问题解决的具体处理建议和措施，经主管签字同意后，交实施人员进行解决方案的实施。服务人员确认是否解决，并将解决方法附在系统缺陷类问题提交单上反馈给问题提出人员。

(4) 问题上报。服务人员收到经业务或技术人员确认的系统缺陷类问题提交单后，上报上级部门。

(5) 问题回复。服务人员根据提交的问题进行分析，制定解决方案并进行实施解决，同时做好变更记录。将解决方案汇总后及时向问题提交单位或问题交办客户作出回复，并将分析过程和问题产生原因一并提交。

第 5 章 项目实施进度

5.1 项目建设周期

本项目建设周期约为 10 个月。

5.2 实施进度计划

培训工作贯穿于项目建设的全过程。

1、 项目实施阶段

时间计划：6 个月

主要任务：在完成总体规划阶段的基础上，根据总体设计方案，进行网络、应用、安全，等保咨询，测评等建设实施的过程。其中应用系统在逻辑上包含众多业务，根据这些业务的内在关系，并考虑整个信息化工作的均衡局面，采用分阶段，有重点的原则进行逐步建设，优先完成技术成熟以及基础核心的应用子系统的相关测评工作。

第 6 章 项目预算

6.1 资金预算总表

等保二级咨询与测评涉及硬件与软件两部分

1. 更换我馆故障频发的防火墙一台
2. 新增系统服务端防勒索，防病毒，EDR 软件
3. 新增专业 web 防火墙一台
4. 利旧沿用我馆已经采购并符合等保二级标准的 IPS 防入侵设备
5. 信息安全等级保护系统测评伍套

本次项目预算经费约为：57.93 万元

产品线	产品名称	规格型号	产品说明（等保二级必选项）	购买数量	自带数量	单位	含税单价（元）	分项含税总价(元)

EDR 新版本(3.5.24 及以上版本)	深信服终端安全管理系统软件 V3.0(产品控制中心)	-	性能参数：最大支持管控 EDR 客户端数量：纯内网场景或者 2000 点以上。 安全策略模板一体化设置，全网资产盘点与风险可视，自动化日志可视化报表一键导出，管理账号分权分域，总分平台级联控制；管理平台需搭配客户端软件一齐使用，单独购买无效，含 1 年升级维护费用	1	0	套	100.00	100.00
	深信服端点安全软件 V3.0(服务器旗舰版)	服务器旗舰版	服务器旗舰版包括： 周密防护：系统漏洞扫描，补丁修复管理、终端基线检查，资产盘点，资产主动发现，微隔离、轻补丁漏洞免疫； 全面防护：文件实时监控，勒索诱饵防护，勒索病毒立体防护，勒索攻击对抗，无文件攻击防护，停更系统智御，远程登录认证（强力防勒索），可信进程防护（强力防勒索），关键目录防篡改（强力防勒索）； 灵敏检测：恶意文件检测，僵尸网络检测，暴力破解检测，网端联动杀毒，WebShell 检测； 快速响应：文件急速隔离，终端一键隔离，感染文件修复，病毒处置响应，网端深度联动（SIP、AF、AC），全网威胁定位； 简便运维：外设管控；	16	0	套	1,080.00	17,280.00
	软件升级	-	年，（默认一年服务）提供购买设备的软	0	1	年	0.00	0.00

	（服务器端）		件升级授权，包括产品版本升级，安全云脑在线分析，人工智能算法模型更新，病毒库轻补丁库更新，引擎特征升级等					
WAF	WAF-1000-B1400 标准产品	WAF-1000-B1400	性能参数：网络层吞吐量：6Gbps，HTTP 应用层吞吐量：430Mbps，HTTP 新建连接数：60000，HTTP 并发连接数：1800000。硬件参数：规格：1U，内存大小：4G，硬盘容量：128GB minisata SSD，电源：单电源，接口：6 千兆电口+4 千兆光口 SFP。功能描述：深信服 Web 应用防火墙专注于网站及 Web 应用系统的应用层安全防护，解决传统安全产品如网络防火墙、IPS、UTM 等安全产品难以应对应用层深度防御的问题。产品具备 Web 应用防护功能、云端订阅功能（需单独购买）。	1	0	台	6,600.00	6,600.00
	深信服 Web 应用防护系统软件 V8.0	适用于 WAF-1000-B1400	系统软件 注：WAF（仅 8.0.7、8.0.23 版本支持防篡改功能）对应防篡改客户端支持服务器版本情况 Windows 2003 32/64bits Windows 2008 32/64bits Windows 2012 64bits CentOS 5/6/7 64bit RHEL 5/6/7 64bit	1	0	套	49,700.00	49,700.00

			Debian 6/7 64bit Ubuntu 10.04-14.4 64bit					
	产品质保	-	年，（默认一年服务）提供购买设备的返厂寄修服务	0	1	年	0.00	0.00
	软件升级	-	年，（默认一年服务）提供购买设备的软件升级授权	0	1	年	0.00	0.00
AF-FH全行业型号（新）	AF-1000-FH1600B标准产品	AF-1000-FH1600B	性能参数：网络层吞吐量：4G，应用层吞吐量：2G，防病毒吞吐量：600M，IPS 吞吐量：600M，全威胁吞吐量：450M，并发连接数：200 万，HTTP 新建连接数：6 万，SSL VPN 推荐用户数（单独购买）：20，SSL VPN 最大用户数（单独购买）：60，SSL VPN 最大理论加密流量（单独购买）：160M，IPSec VPN 最大接入数：300，IPSec VPN 吞吐量：270M。 硬件参数：规格：1U，内存大小：4G，硬盘容量：128G SSD，电源：单电源，接口：8 千兆电口+2 千兆光口 SFP。	1	0	台	4,200.00	4,200.00
	深信服防火墙软件基础级	适用于AF-1000-FH1600B	产品出厂默认自带功能，包括 ACL 控制、应用识别与流控、入侵防御、僵尸网络检测等功能	1	0	套	21,220.00	21,220.00

	深信服防火墙软件增强级模块	适用于AF-1000-FH1600B	下一代应用防火墙软件增强级功能模块授权购买费用	1	0	套	2,550.00	2,550.00
	网关杀毒升级许可	网关杀毒更新	购买杀毒功能模块后每年更新费用	1	0	套	2,550.00	2,550.00
	网关杀毒模块（不含1年更新）	网关杀毒模块	模块授权购买费用，不含网关杀毒更新注：本地杀毒功能模块收取一次开通费用，永久有效。未购买杀毒更新，杀毒功能仍然有效，病毒库无法更新。	1	0	套	2,550.00	2,550.00
	深信服云智订阅软件（AF8.0.7及以上版本适用）	适用于AF-1000-FH1600B	按年收费,包括WEB应用防护识别库、IPS特征库、僵尸网络防护库、实时漏洞分析识别库和URL&应用识别库定期更新，保持设备具备检测防御最新威胁的能力。	1	0	套	2,550.00	2,550.00
	产品质保	-	年，（默认一年服务）提供购买设备的返厂寄修服务	0	1	年	0.00	0.00
	软件升级	-	年，（默认一年服务）提供购买设备的软件升级授权	0	1	年	0.00	0.00
等保二级测评	等保二级等保服务		评测单位（上海计算机软件技术开发中心） 收费标准 每系统（复测评，市网安）		2	系统	55,000.00	110,000.00
等保三级测	等保三级测评		评测单位（上海计算机软件技术开发中		3	系统	90,000.	270,000.0

评		心） 收费标准 每系统（新系统测评，市网安）				00	0
等保三级信息系统安全咨询	等保三级信息系统安全咨询	等保三级信息安全咨询服务单位（上海计算机软件技术开发中心）（复测系统重新信息安全评估一套，新系统信息安全咨询评估二套）（1年系统信息安全咨询服务）		3	系统	30，000.00	90，000.00
总价：伍拾柒万玖仟叁佰元整							579,300.00

第 7 章 项目效益

7.1 促进全面提升网络信息安全保障

探索运用先进网络技术为监管技术支撑提供安全智能化应用和服务，优化工作效率、事中监测的监管工作模式，辅助工作人员监督，提高网络安全水平，提高整体效率，降低信息安全风险，提高主动发现问题能力和监管智能化水平，保障网络信息安全的可持续发展。

第 8 章 项目效益

8.1 促进全面提升网络信息安全保障

探索运用先进网络技术为监管技术支撑提供安全智能化应用和服务，优化工作效率、事中监测的监管工作模式，辅助工作人员监督，提高网络安全水平，提高整体效率，降低信息安全风险，提高主动发现问题能力和监管智能化水平，保障网络信息安全与外聘技术支撑双活模式创新。