一、网络安全等级保护

《中华人民共和国网络安全法》第二十一条规定网络运营者应当按照网络安全等级保护制度的要求，履行相关的安全保护义务。同时第七十六条定义了网络运营者是指网络的所有者、管理者和网络服务提供者。网络（个人与家庭网络除外）运营者必须按网络安全法开展等级保护工作。

什么是网络安全等级保护

等级保护是指根据信息系统应用业务**重要程度**及其实际安全需求，实行**分级**、分类、分阶段实施保护，按标准进行建设、管理和监督，保障信息安全和**系统**安全正常运行，维护国家利益、公共利益和社会稳定。国家对信息安全等级保护工作运用法律和技术规范逐级加强监督监管力度。突出重点、保障重要信息资源、重要信息系统的安全。

网络安全对企业的影响

1、各大网站数据泄露频发、舆情、不合规，我们企业有什么责任。

对收集的用户严格保密，并建立健全的用户信息保护机制，不得非法收集、提供、获取、使用用户信息。

2、我们需要承担什么样的后果？

侵害个人隐私=违法

情节严重会停业整改或吊销营业执照

主体负责人罚款

网络安全运营者应对**报障用户信息安全**负有主要责任

为什么要做等保

01 满足相关部门合规要求

02 建立网络安全防护体系

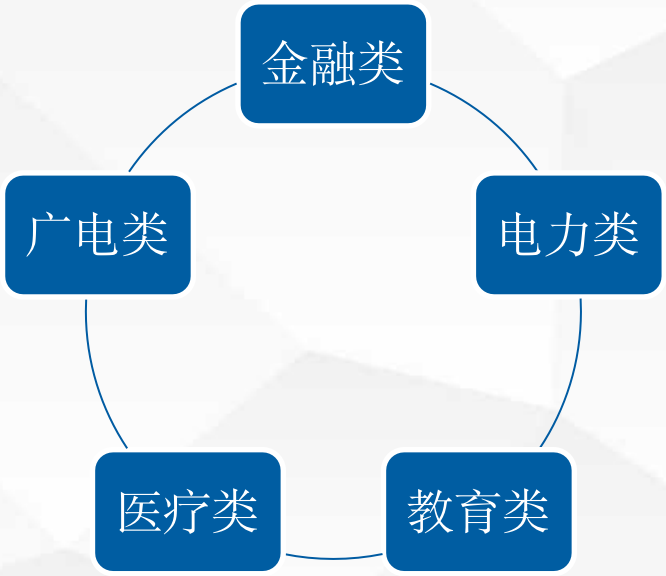
03 主管单位要求行业用户开展等保工作

04 合理规避风险

05 企业上市准备

06 提升企业形象，增强产品和行业竞争力

哪些行业要求做



目前已经下发行业要求文件的有：金融、电力、广电、医疗、教育等行业，还有一些行业主管单位要求行业客户开展等级保护工作。

等保2.0的相关要求

1、安全技术要求（安全策略调整、安全设备部署）

- 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

2、安全管理要求（安全制度体系、日常工作日志整理）

- 安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理

等保要怎么做


01
系统定级
确定定级对象，初步确认定级对象，专家评审，主管部门审核。
02
系统备案
持定级备案和备案表前往当地公安网监部门进行备案。
03
建设整改
参照定级对象当前等级要求和标准，对定级对象进行整改加固。
04
系统评测
委托当地测评机构，对系统进行全面测评，出具测评报告。
05
监督检查
系统持续改进与优化，并按照相关要求进行年检。

行业定级标准

信息系统		建设目标	
××网站平台		×级等保测评	
对客体的伤害程度			
受伤害的客体	一般损害	严重损害	特别严重损害
公民、法人、其他组织的合法权益	第一级	第二级	第三级
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

行业定级标准

等级	等级定义	系统
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；	个人网站、不影响社会的业务
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	普通网站、教育、小门户、公司平台等
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	互联网、大型企业、金融行业非银机构等
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	银行核心、电力调度等
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。	

评测周期

网络安全等级保护办法

第二级：每2年一次

第三级：每年至少一次

第四级：每年至少一次

第5级：依据特殊安全需求测评

等保测评流程及周期

实施步骤	实施内容	成果	实施方	时间
定级	根据被测系统本身的系统服务和业务数据进行定级，编写定级材料	备案表、定级报告、自查表、备案电子表单等材料	测评单位和被测单位	一周
公安网警首次备案	提交备案表、定级报告、自查表、备案电子表单等材料进行备案	备案编号	测评单位	提交材料后大约需要一周(取决于公安处理效率)
测评资料准备	准备等保管理制度和记录文档	等保管理制度和记录文档	被测单位为主，测评单位提供模板	取决于客户
现场测评	技术测评和管理测评，技术测评包括网络、主机、数据库、应用系统等层面的安全检查和测评	测评记录	测评单位为主被测单位配合	2-7天现场测评，取决于系统的复杂程度，以及服务器、网络设备、安全设备的数量
整改	被测单位整改，整改完成测评单位实施复测		被测单位整改，测评单位提供整改建议及复测评	时间进度取决于被测单位，对于存在高风险的项目整改之后需要复测
出具报告	测评单位出具等保测评报告	等保测评报告	测评单位	7-15天
公安网警二次备案	提交等保测评报告、整改报告等材料	备案证明	测评单位为主被测单位配合	提交材料后大约需要两周(取决于公安处理效率)

安全产品服务清单

二级等保合规加固版安全产品（服务）列表	
下一代防火墙（**必选**）	日志审计系统（**必选**）
网络防病毒系统（**必选**）	堡垒机（**必选**）
数据库审计（**必选**）	检测探针+感知平台（可选）
SSL VPN（建议选择）	上网行为管理（建议选择）
互联网业务安全托管服务（可选）	风险评估服务（可选）

安全产品服务清单

三级等保合规加固版安全产品（服务）列表	
下一代防火墙（**必选**）	日志审计系统（**必选**）
网络防病毒系统（**必选**）	上网行为管理（**必选**）
数据库审计（**必选**）	堡垒机（**必选**）
检测探针+感知平台（**必选**）	SSL VPN（建议选择）
负载均衡（建议选择）	基线核查系统（建议选择）
互联网业务安全托管服务（建议选择）	邮件安全网关（建议选择）
广域网优化设备（可选）	风险评估服务（可选）
渗透测试服务（可选）	应急响应及应急演练服务（可选）

等保一站式服务

等保一站式服务优势


节约时间
与国内知名专业测评机构及安全厂家合作，咨询、整改同步进行，缩短等保建设时间
节约成本
比单独选择咨询、测评以及整改服务成本低，无需投入大量人力参与等保建设中，节约公司的各项成本
客户省心
由工程师全程一对一对接参与，等保建设全程辅导跟踪，客户只需投入极少的人力配合

整改服务：差距评估

差距评估过程

1、确定等级保护对象的基本安全需求

2、选择调整基本安全需求

3、明确特殊安全需求

4、根据各项安全要求逐项分析

差距评估方法

1、人工检查

2、漏洞扫描

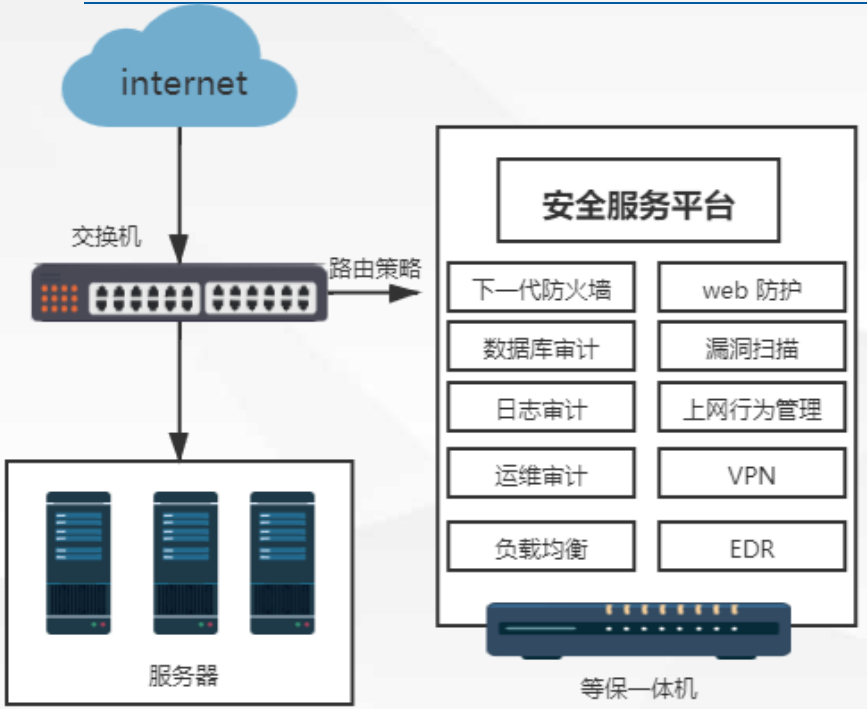
3、渗透测试

4、网络架构分析

5、安全访谈

6、管理制度评估

整改服务：方案设计



1、以“一个中心、三层防护”为模型进行分区域涉及，保障设计方案的合规性

2、结合安全、动态、防御三种能力建立防御体系，提供持续性安全保护。

3、结合运维等人性化技术手段，让安全运维管理更加简单高效、更合规。

云上等保产品

整改服务：整改实施

1、安全设备采购部署

根据设计方案内容，协助用户单位完成安全设备的采购和部署。

2、安全管理制度整理

根据差距评估的结果，针对用户单位目前缺少的安全管理制度进行补充，完成安全管理支付汇编。

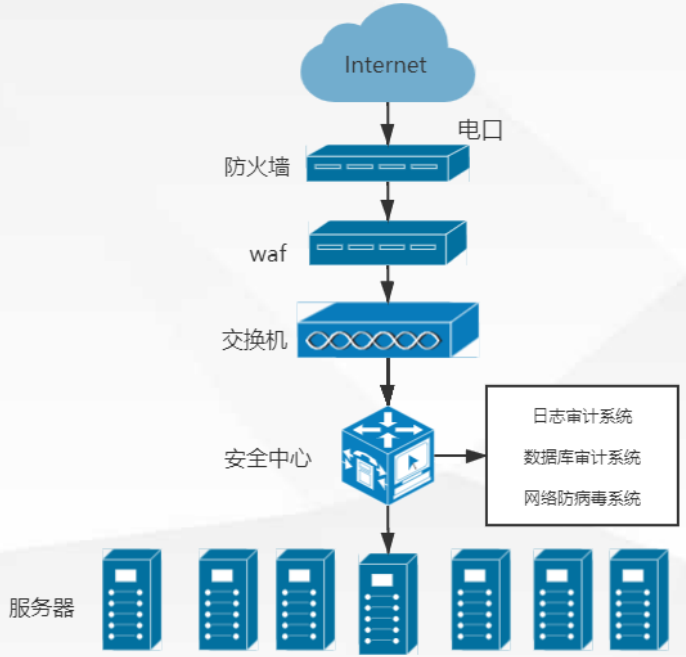
3、安全策略配置

针对用户单位实际情况和等级保护要求，制定相关设备的安全策略要求，并合理配置。

4、安全加固

针对差距评估中自身安全策略配置不当和版本补丁问题进行处理，包括调整自身安全策略、升级版本和打补丁。

等保二级用户案例



客户名称：浙江**信息咨询股份有限公司

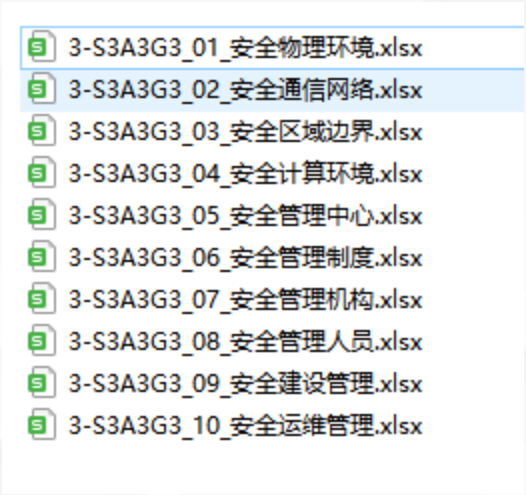
定级：二级

该用户于2021年4月托管至我司兴议电信机房

谢　谢

网鼎科技

建设整改内容


3-S3A3G3_01_安全物理环境.xlsx
3-S3A3G3_02_安全通信网络.xlsx
3-S3A3G3_03_安全区域边界.xlsx
3-S3A3G3_04_安全计算环境.xlsx
3-S3A3G3_05_安全管理中心.xlsx
3-S3A3G3_06_安全管理制度.xlsx
3-S3A3G3_07_安全管理机构.xlsx
3-S3A3G3_08_安全管理人员.xlsx
3-S3A3G3_09_安全建设管理.xlsx
3-S3A3G3_10_安全运维管理.xlsx

杭州等保测评机构

浙江等级保护测评机构查询

国家网络安全等级保护工作协调小组办公室推荐测评机构名单		
DJCP2010330086	浙江省电子信息产品检验研究院	浙江省杭州市天目山路50号信息技术大厦
DJCP2010330087	浙江省发展信息安全测评技术有限公司	浙江省杭州市环城西路33号
DJCP2010330088	杭州安信检测技术有限公司	浙江省杭州市滨江区长河路590号4幢2楼A1-A18、B1-B12座
DJCP2010330089	浙江鑫诺检测技术有限公司	浙江省宁波市鄞州区中河街道天童北路933号和邦大厦A座2208室
DJCP2010330090	浙江东安检测技术有限公司	浙江省杭州市西湖区莲花街333号莲花商务中心A座11楼
DJCP2011330091	浙江安远检测技术有限公司	浙江省金华市丹溪路1171号龙腾创业大厦1001室
DJCP2014330092	浙江辰龙检测技术有限公司	浙江省杭州市萧山区宁围街道民和路481号联合中心南区1102室
DJCP2014330093	浙江方圆检测集团股份有限公司	浙江省杭州市江干区幸福南路115号