网络安全等级保护硬件及软件要求-二级、三级等保系统要求

产品名称	网络安全等级保护硬件及软件要求- 二级、三级等保系统要求
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

产品详情

第一部分：二级网络安全等级保护要求

(一)机房方面的安全措施需求：

1、防盗报警系统

2、灭火设备和火灾自动报警系统

3、水敏感检测仪及漏水检测报警系统

4、精密空调

5、备用发电机

(二)主机和网络安全层面需要部署的安全产品：

1、防火墙或者入侵防御系统

2、上网行为管理系统

3、网络准入系统

4、审计平台或者统一监控平台(可满足主机、网络和应用层面的监控需求，在条件不允许的情况下，至少要使用数据库审计)

5、防病毒软件

(三)应用及数据安全层面需要部署的安全产品：

1、VPN

2、网页防篡改系统(针对网站系统)

3、数据异地备份存储设备

4、主要网络设备、通信线路和数据处理系统的硬件冗余(关键设备双机冗余)。

第二部分：三级网络安全等级保护的要求

一、机房方面的安全措施需求：

1、需要使用彩钢板、防火门等进行区域隔离

2、视频监控系统

3、防盗报警系统

4、灭火设备和火灾自动报警系统

5、水敏感检测仪及漏水检测报警系统

6、精密空调

7、除湿装置

8、备用发电机

9、电磁屏蔽柜

二、主机和网络安全层面需要部署的安全产品：

1、入侵防御系统

2、上网行为管理系统

3、网络准入系统

4、统一监控平台(可满足主机、网络和应用层面的监控需求)

5、防病毒软件

6、堡垒机

7、第二代防火墙或防火墙

8、审计平台(满足对操作系统、数据库、网络设备的审计，在条件不允许的情况下，至少要使用数据库审计)

三、应用及数据安全层面需要部署的安全产品：

1、VPN

2、网页防篡改系统(针对网站系统)

3、数据异地备份存储设备

4、主要网络设备、通信线路和数据处理系统的硬件冗余(关键设备双机冗余)。

5、数据加密软件(满足加密存储，且加密算法需获得保密局认可)。

第三部分：网络安全等级保护需要用到的设备

1. 电子门禁系统

物理访问控制

重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

2. 房防盗报警系统/监控报警系统

防盗窃和防破坏

应利用光、电灯技术设置机房防盗报警系统;

应对机房设置监控报警系统。

3. 火灾自动消防系统

防火

机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火。

4. 水敏感检测设备

防水和防潮

应安装队水敏感的检测仪表活元件，对机房进行防水检测和报警。

5. 机房专用空调

温湿度控制

机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。

6. UPS或备用发电机

电力供应

应建立备用供电系统。

7. 负载均衡

结构安全

应保证网络各个部分的带宽满足业务高峰需要;

应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。

8. 防火墙

访问控制(网站系统，需部署web应用防火墙、防篡改系统。)

应在网络边界部署访问控制设备，启用访问控制功能;

应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;

应对进出网络的信息内容进行过滤，实现对应用层HTTP、FTP、TELNET、SMTP、POP3等协议命令级的控制。

9. 准入准出设备

边界完整性检查

应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;

应能够对内部网络用户私自联到外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。

10. IDS/IPS

入侵防范

应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;

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应提供报警。

11. 防病毒网关(或UTM、防火墙集成模块)

恶意代码防范

应在网络边界处对恶意代码进行检测和清除;

应维护恶意代码库的升级和检测系统的更新。

12. 日志审计系统/数据库审计系统日志服务器

安全审计

应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;

审计记录应包括：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;

应能够根据记录数据进行分析，并生成审计报表;

应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;

数据库安全审计

审计范围应覆盖到服务器和重要客户端上的每个操作系统用户和数据库用户;

审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件;

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;

应能够根据记录数据进行分析，并生成审计报表;

应保护审计进程，避免收到未预期的中断;

应保护审计记录，避免受到未预期的删除、修改或覆盖等。

13. 网络版杀毒软件

恶意代码防范

应安装防恶意代码软件，并及时更新恶意代码软件版本和恶意代码库;

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;

应支持防恶意代码软件的统一管理。

14. 运维管理系统

资源控制

应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;

应限制单个用户对系统资源的最大或最小使用限度;

应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

15. 堡垒机+UKey认证

网络设备防护

主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别;

身份鉴别

应采用两种或两种以上组合的鉴别技术来管理用户进行身份鉴别;

应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。

16. 数据备份系统/异地容灾

备份和恢复

应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放;

应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地。

17. 漏洞扫描设备

网络安全管理

应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;

系统安全管理

应定期进行漏洞扫描,对发现的系统安全漏洞及时进行修补。