附件 2

属地企业网络安全防护指南

一、企业网站及业务系统安全防护建议

为加强企业门户网站及业务信息系统的网络安全防护，降低遭受网络攻击篡改的风险，建议采取以下防护措施：

1.配置网络防火墙或购买云防护服务，可监控过滤外部网络访问流量，阻止未经授权的访问和恶意攻击。

2.用户登录应采取多因素身份验证措施，如指纹、短信验证码或硬件令牌来提供额外保护。

3.强制实施强密码策略，确保所有用户都使用复杂且不易推测的密码，坚决杜绝弱口令问题，并定期提醒更换密码。

4.网站或业务信息系统更换管理员时，需及时更改相应的系统管理和数据管理密码。

5.严格控制对重要敏感数据和系统资源的访问权限，要按照最小化原则分配用户权限级别。对于应用类网站可限制其访问的IP 地址来限制访问范围。

6.定期更新和修补系统，第一时间安装操作系统和应用程序的最新安全补丁及更新，以及时修复已知漏洞隐患。

7.针对网站或业务信息系统涉及的中间件、数据库、平台组件等程序应保证及时进行安全补丁升级。

8.信息系统或应用程序上线前进行安全审计、代码扫描和漏洞测试，严防“带病上岗”。确保启用安全日志审计功能，记录

存储时间需超过6个月。

9.定期对企业网站通过漏洞扫描、渗透测试等方式进行安全检测，以便及时发现和纠正潜在的安全问题。

10.网站系统使用SSL/TLS协议对重要敏感数据进行加密传输，以保护数据的机密性和完整性。

11.有条件的企业可部署入侵检测和防御系统，及时检测和阻止潜在的入侵行为。

12.业务数据重要的企业，应定期备份重要数据到安全地方，同时建立灾难恢复计划，以便在遭受攻击或故障时快速恢复业务数据。

13.一旦发生被攻击篡改事件或发现有害信息，迅速落实断网断电并拨打110报案。

二、企业移动应用程序（小程序）安全防护建议

为了保护企业移动应用程序（小程序）的使用运营安全，建议采取以下防护措施：

1.在移动应用程序（小程序）的开发和测试阶段，应考虑安全编码、验证输入、限制访问、防止SQL注入等安全性，并遵循安全最佳实践。

2.用户登录时应采取多因素身份验证、单点登录等身份安全认证机制，确保只有授权用户可以访问和使用。

3.对移动应用程序（小程序）传输的重要敏感数据使用SSL/TLS协议等进行加密，防止数据在传输过程中被窃取或篡

改。

4.对移动应用程序（小程序）的重要敏感数据进行加密存储，并实施数据访问权限控制措施，确保数据的机密性和完整性。

5.随时跟踪移动应用程序（小程序）开发者发布的安全更新和修复程序，及时修补已知漏洞隐患。

6.使用加密通信协议和数字证书，确保移动应用程序（小程序）与后端服务器之间的通信是安全的，防止数据被窃取或篡改。

7.做好移动应用程序（小程序）操作访问的监视分析，及时检测发现异常行为和潜在的安全威胁，并采取相应防御措施。

8.定期通过漏洞扫描、渗透测试等方式对移动应用程序（小程序）进行安全评估，以便及时发现和纠正潜在的安全问题。

9.建立网络安全应急预案及应急响应计划，明确应对紧急事件的流程和联系人，以快速应对和处置网络安全事件。

10.一旦发生被攻击篡改事件或发现有害信息，迅速落实断网断电并拨打 110 报案。

三、企业联网显示屏安全防护建议

为确保企业（包含分支机构或连锁门店）的联网显示屏内容播出安全，建议采取以下防护措施：

1.通过安装在安全位置、使用锁定装置或监控摄像头等方式来保证联网显示屏设备物理安全，避免非授权人员直接接触操作设备。

2.使用如密码+手机短信、指纹识别或数字证书等强身份验

证机制，同时指定特定 ip 访问等策略来限制对联网显示屏的管理权限，确保只有授权人员能够访问和控制显示屏管理后台及设备。

3.定期更新和维护联网显示屏的系统软件和应用程序，并安装最新的安全补丁及更新，以修复已知漏洞。

4.采用 HTTPS 等安全加密协议来保证联网显示屏和后端服务器之间的加密通信，防止数据被窃取或篡改。

5.定期通过漏洞扫描、渗透测试等方式对联网显示屏后台管理系统进行安全检测评估，以便及时发现后门木马等潜在安全问题。

6.定期进行联网显示屏后台管理系统的安全审计和监控，检测发现和应对处置异常账号、异常访问等威胁行为。

7.要对联网显示屏发布推送内容要严格审核把关，确保不出现涉赌涉黄涉政等违规有害信息。

8.加强联网显示屏管理主机终端的安全管理，安装最新版杀毒软件定期查杀，杜绝使用弱口令，同时加强对使用管理联网显示屏的人员的网络安全教育培训，识别与应对各类网络钓鱼陷阱，严防管理主机终端被攻击控制。

9.非必需联网的显示屏可采取本地局域网形式进行显示内容投放管理，杜绝来自互联网侧的网络安全威胁。

10.一旦发生被攻击篡改事件或发现有害信息，迅速落实断网断电并拨打 110 报案。

四、企业办公终端安全防护建议

为确保企业办公终端电脑的网络安全，建议采取以下防护措施：

1.操作系统登录账户需要设置登录密码，且不为弱密码。

2.操作系统应及时更新最新安全补丁。

3.禁止开启无权限的文件共享服务，使用更安全的文件共享方式。

4.关闭操作系统中不需要的服务，特别是要关闭远程访问等高危端口。

5.定期备份重要文件及数据。

6.安装病毒防护程序并更新最新病毒特征库。

7.不随意点击来历不明的链接或下载安装未经安全严重的软件程序。

8.员工离开座位时应设置电脑为退出状态或锁屏状态，建议设置自动锁屏。

9.加强企业员工网络安全意识教育，培训识别和应对各种网络威胁，要严防网络钓鱼攻击，切不可打开来历不明的电子邮件附件及 QQ、微信等社交聊天工具发送的程序、文档。