学校网络安全年度工作总结

汇报人：XXX

汇报时间：2023-12-31

目录

01

工作概况

工作目标

保障学校网络系统的安全稳定运行，防止信息泄露、篡改和破坏。

提高学校师生网络安全意识，加强网络安全培训和教育。

完善网络安全管理体系，建立有效的安全监测和应急响应机制。

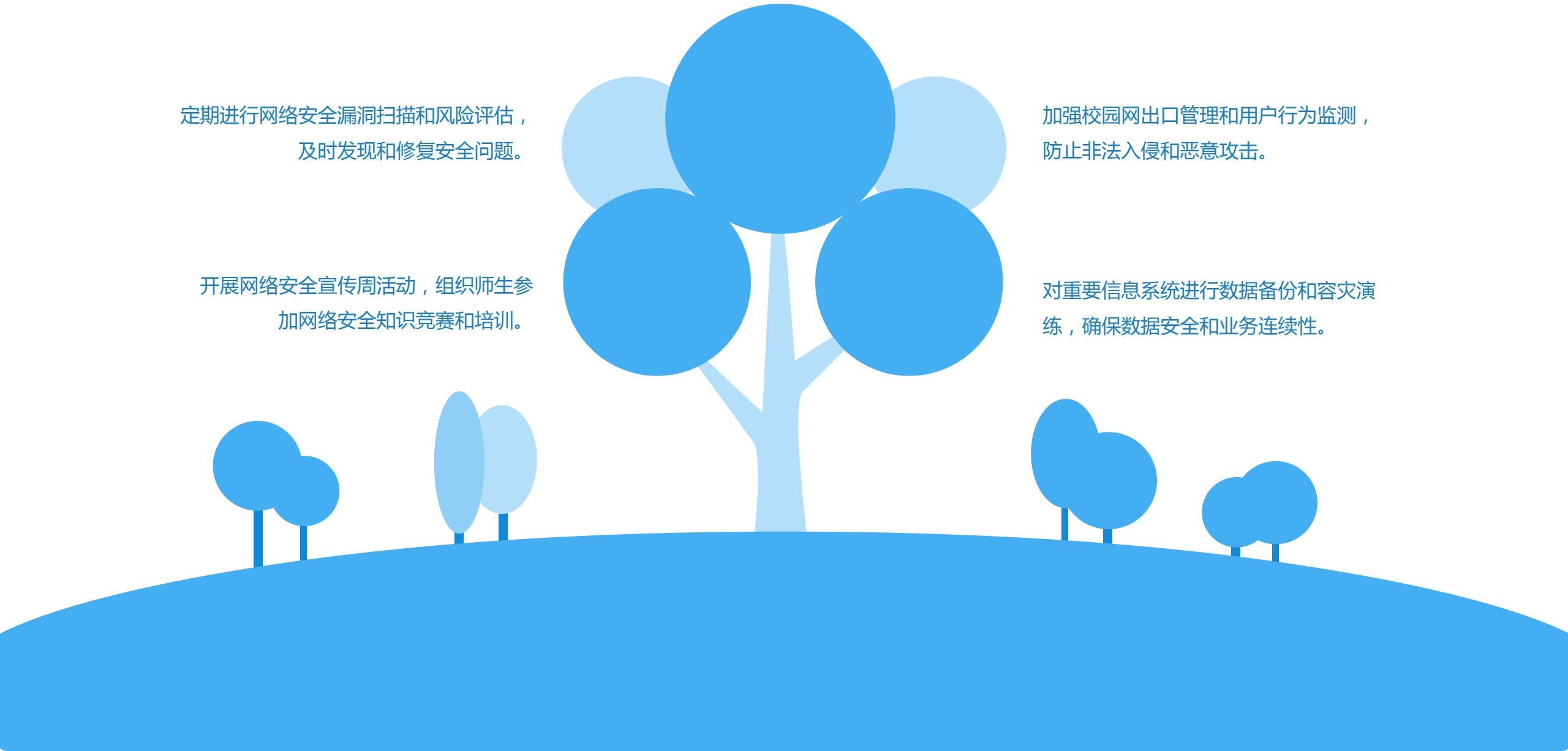
工作内容

定期进行网络安全漏洞扫描和风险评估，及时发现和修复安全问题。

加强校园网出口管理和用户行为监测，防止非法入侵和恶意攻击。

开展网络安全宣传周活动，组织师生参加网络安全知识竞赛和培训。

对重要信息系统进行数据备份和容灾演练，确保数据安全和业务连续性。



工作成果

学校网络系统安全稳定运行，未发生重大安全事件和数据泄露事件。

01

提高了学校师生的网络安全意识和技能水平，有效减少了网络诈骗和病毒攻击的风险。

02

完善了网络安全管理体系，建立了较为健全的安全监测和应急响应机制。

03

获得了上级主管部门的表扬和肯定，为学校赢得了良好的社会声誉。

04

05

02

安全防护工作

防火墙配置

01

防火墙规则更新

定期检查并更新防火墙规则，以应对新型网络威胁和攻击。

02

访问控制策略

根据学校网络需求，制定合理的访问控制策略，限制不必要的网络流量和访问。

03

端口安全

对常用端口进行安全配置，防止潜在的攻击和恶意流量。

入侵检测与防御

01 02 03

入侵检测系统部署

配置入侵检测系统，实时监测网络流量，发现异常行为及时报警。

威胁情报共享

与安全厂商合作，获取最新的威胁情报，提高防御能力。

安全事件响应

建立安全事件响应机制，对发现的攻击行为进行及时处置和溯源。

数据备份与恢复

01

数据备份策略

制定完善的数据备份策略，确保重要数据得到及时备份。

02

备份数据验证

定期验证备份数据的完整性和可用性，确保在需要时可以顺利恢复。

03

数据恢复演练

定期进行数据恢复演练，提高数据恢复的效率和准确性。

病毒防范与处理

防病毒软件部署

安装可靠的防病毒软件，对病毒、木马等恶意程序进行实时监测和清除。

安全培训与意识提升

开展网络安全培训和宣传活动，提高师生网络安全意识和防范能力。

安全漏洞修复

及时修复系统和软件的安全漏洞，降低被攻击的风险。

03

安全事件处置