

网络安全服务外包第三方服务管理办法（试行）

第一章 总则

第一条 为规范学院信息化建设工作，提升学院网络安全和数据安全管理水平，确保教学管理正常进行，特制定本办法。

第二条 本办法适用于职业学院与第三方网络安全公司（以下简称“服务商”）开展的网络安全服务外包活动。

第三条 学院应确保与服务商签订的合同和协议明确双方的权利和义务，并符合相关法律法规和学院规章制度的要求。

第二章 网络安全服务要求

第四条 服务商应提供全面的网络安全服务，包括但不限于网络安全监测、漏洞扫描、应急响应、安全培训、技术咨询等。

第五条 服务商应定期对学院网络系统进行安全检查和风险评估，及时发现并修复安全隐患。

第六条 服务商应提供网络安全事件应急响应服务，确保在发生网络安全事件时能够及时响应并处置。

第三章 数据安全要求

第七条 服务商在处理学院数据时，应严格遵守《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》

《中华人民共和国保守国家秘密法》《网络数据安全管理条例》，确保数据的保密性、完整性和可用性。

第八条 服务商应建立完善的数据备份和恢复机制，定期对数据进行备份，确保在数据丢失或损坏时能够及时恢复。

第九条 服务商应提供数据加密和访问控制服务，确保数据在传输和存储过程中的安全性。

第四章 技术服务与 7*24 小时响应

第十条 服务商应提供全天候（7*24 小时）的技术支持服务，确保在学院遇到网络安全问题时能够迅速响应并提供解决方案。

第十一条 服务商应设立专门的技术支持团队，负责处理学院的网络安全咨询、技术支持和故障排查等工作。

第十二条 服务商应提供定期的技术培训和知识分享与培训，提升学院教职工和学生的网络安全意识和技能。

第五章 服务监督与考核

第十三条 学院应建立服务监督和考核机制，定期对服务商提供的服务进行评估和考核。

第十四条 学院应根据服务监督和考核结果，及时调整服务内容和合作方式，优化服务流程和提高服务效率。

第十五条 学院应定期对服务商的服务质量进行满意度调查，了解教职工和学生的需求和意见，不断改进服务质量。

第六章 保密与违约责任

第十六条 学院与服务商应签订《网络安全服务保密协议》，明确双方在信息安全方面的责任和义务，防止信息泄露和滥用。

第十七条 若服务商违反合同条款或法律法规，给学院造成损失的，应承担相应的违约责任。

第七章 附则

第十八条 本办法由网络综合治理、网络安全和信息化领导小组办公室负责解释和修订。

第十九条 本办法自发布之日起施行，原有相关规定与本办法不符的，以本办法为准。

附件 1：网络安全服务保密协议

网络安全服务保密协议

甲方（服务接受方）：

乙方（服务提供方）：

甲乙双方经友好协商，根据《中华人民共和国民法典》及相关法律法规的规定，就乙方在为甲方提供安全服务的过程中可能获悉的甲方保密信息及为甲方保密事宜，达成如下协议：

1. 本协议所称“保密信息”是指：乙方基于为甲方提供安全服务所获取的甲方域名、业务系统等虚拟资产中所附带的或甲方安全设备上报的网络安全信息以及用户数据和业务相关信息等。

2. 未经甲方书面同意，乙方不得以任何形式或任何方式将保密信息和/或其中任何部分，泄漏或透露给任何第三方。乙方有义务妥善保管保密信息，不得擅自复制备份，并应避免泄露或遗失。乙方亦不得依据保密信息，就任何问题，向任何与甲方所需安全服务无关的第三方做出任何建议。

3. 甲方同意乙方有权因提供服务的必要，而向其安全服务人员透露或允许其接触保密信息和/或其中的任何部分，同时，乙方承诺该等服务人员在提供服务的过程中将对其所接触的保密信息承担与本协议同等的保密义务。

4. 甲方有权在服务终止时要求乙方将所获悉的保密信息归还给甲方，不能归还的，应进行销毁处理。

5. 凡因执行本协议所发生的或与本协议有关的一切争议，双方应通过友好协商解决。如果协商不能解决时，任何一方可向被告所在法院提起诉讼。

6. 本协议保密期限为整个安全服务期间以及服务期限截止后两年。

7. 本协议一式两份，自双方盖章之日起生效。

甲方：

乙方：

（章印）

（章印）

日期：

日期：