上海震旦职业学院信息安全管理体系

网络安全管理制度

修改记录

日期	版本	作者/修改者	修订类型	描述
2014-12-20	1.0	程茂华	创建	创建全页
2015-02-23	1.1	程茂华	修改	结合实际情况修订第八章--网络设备安全管理第三十一条和第九章--网络保密管理的第三十七、四十二条规定

目 录

第一章　总则

第一条　为加强对上海震旦职业学院信息中心网络系统的安全管理，确保上海震旦职业学院网络系统的安全运行，制定本办法。

第二条　本办法所指网络系统分为公共上网网络和邮件服务器上网网络。

第三条　上海震旦职业学院信息中心的运维部为技术支持中心，负责上海震旦职业学院信息中心网络系统的建设升级、运行维护和安全管理工作。

第二章　网络拓扑管理

第四条　网络整体的拓扑结构需进行严格的规划、设计和管理，一经确定，不能轻易更改。

第五条　如因业务需要，确需对网络的整体拓扑结构进行调整和改变，需按照相应的变更与管理规程上报。

第六条　公共上网区和内部上网区，使用防火墙等安全设备以及 VLAN 或其他访问控制方式进行分离。

第七条　网络结构要按照分层网络设计的原则来进行规划，合理清晰的层次划分和设计，可以保证网络系统骨干稳定可靠、接入安全、便于扩充和管理、易于故障隔离和排除。

第三章　网络配置管理

第八条　运维部网络管理人员负责对网络系统的统一配置管理工作，未经运维部负责人同意，相关人员无权进行网络系统的网络配置。

第九条　网络部门负责网络的性能分析，以充分了解系统资源的运行情况及通信效率情况，提出网络优化方案。

第十条　所有的网络配置工作都要有文档记录，网络设备的配置文件需要定期备份。

第十一条　按照最小服务原则为每台基础网络设备进行安全配置。

第十二条　网络需保持持续不断的运行，维护工作要在用户使用量小的时候进行。

第四章　网络互连

第十三条　网络按访问控制策略划分为内网和外网。

第十四条　外网访问原则

内网用户不允许访问外网，如工作需要需经信息中心技部审批才能开通外网访问权限；

第五章　终端的接入管理

第十五条　只有安装防病毒软件的计算机终端方能接入办公业务网络和互联网；生产操作终端只能在机房内接入生产网络。

第十六条　终端接入系统时必须通过安全审计部门审批通过后方能接入。

第十七条　终端接入时与上海震旦职业学院信息中心网络隔离，在此电脑的杀毒软件的病毒库

及相应补丁打到最新的状态时进行全面扫描。当所有病毒全部查杀完毕，经网络接入管理人员验证后方可接入。

第六章　网络监控管理

第十八条　安全审计部门和网络部门共同负责网管系统和网络安全的建设和维护，以实现对网络安全情况的实时监控和管理，确保整个网络安全、稳定运行。

第十九条　使用入侵检测、漏洞扫描等设备和技术定期对网络安全情况进行监控和分析，对于监控到的异常行为要有及时、有效的处理机制。

第二十条　在监控过程中，如发现网络异常、严重影响业务的问题，要立即按照事件处理流程向上一级报告。

第二十一条　网络管理员负责网络设备的日常检查，监测网络设备性能参数和网络运行状况；对关键设备要做到每日检查，发现问题应迅速解决，全部管理工作应保留记录。

第二十二条　定期或不定期对备件及备用线路进行检测和维护。

第二十三条　网络安全监控设备的运行不能影响网络的正常使用。

第二十四条　要对所有在线网络设备运行情况记录登记，并定期上报网络运行状况报告。

第七章　网络审计管理

第二十五条　安全审计部门定期对涉及网络配置的增、删、修改等操作的配置更改记录进行审计。

第二十六条　采取必要措施统一日志，安全审计部门定期对日志进行分析，检查违规行为。

第二十七条　要定期对系统用户和管理员的访问权限进行审查。

第二十八条　重要资源的访问控制策略至少要每六个月审计一次。

第八章　网络设备安全管理

第二十九条　所有网络设备或主机都必须有专人负责管理。

第三十条　所有新增网络设备或主机必须先行以文字形式向本部门提交有关信息，经运维部登记并按要求做相应设置，使用人签名办理相关使用手续后使用。

第三十一条　所有连接到静态 IP 网段内的网络设备及主机，需按要求设置设备或主机名称并由其分配 IP 地址；IP 地址一经分配，不得无故更改，因更改而引起的网络连接问题责任自负；如确需修改 IP 地址的，需向运维部提出申请并由其分配新 IP。

第三十二条　所有与上海震旦职业学院信息中心网络相连接的设备都需及时维护，若因维护不及时对生产办公造成影响的，将责令相关部门及责任人立即整改。

第三十三条　所有主机及具有可管理功能的网络设备均应启用日志功能。

第三十四条　所有具备可管理功能的网络设备需手动关闭尚未使用的端口，以防未经授权的设备接入。

第三十五条　所有接入上海震旦职业学院信息中心内网络的设备不得设置为网关或 DHCP 服务

器（经运维部允许的除外），如发现自行设置的网关或 DHCP 服务器，将立即强制停止使用。

第三十六条 网络设备升级、改造、重大调整、停机维护前，需由 xx 银行科技部经理审批。

第九章 网络保密管理

第三十七条 凡使用互联办公网络的部门，必须有一位领导分管并指定专人负责本部门网络节点内安全保密工作，经常进行监督、检查，处理本单位涉及网络安全保密的有关事宜，并协助主管部门开展安全保密工作的检查指导。

第三十八条 网络建设和运行，必须有技术上的安全和保密控制措施，拒绝未经授权的访问。

第三十九条 网络管理用户的口令和采取的安全措施，属于机密级事项；有调阅机密内容权限的用户口令和网络系统级口令及安全措施属于机密事项，不能转告非授权用户。

第四十条 不得在网上擅自连接各类网络设备。所有网络设备的增减与变动，其技术方案必须经过审批，并在网络技术人员的监督下执行。

第四十一条 各部门需要安装主机、服务器等设备时，必须预先报安全审计组核准，并由其进行安全和技术审核，网络工程部分配网络地址和设置安全措施后，方可实施安装。

第四十二条 各单位需要通过互联网与外单位进行信息（含数据）交换，应经过上海震旦职业学院信息中心提供的统一数据交换通道进出。由于特殊原因个别部门要求建立独立的网络信息通道时，应事先报上海震旦职业学院信息中心领导批准并经安全审计组进行内部技术安全审查。