泉州海洋职业学院
网络安全管理制度

制定：安全管理员

审核：信息安全办公室

批准：信息安全领导小组

版本：V1.0

泉州海洋职业学院

二０一八年六月

版本控制

时间	版本	说明	修改人
2018.06.17	V1.0	制度建立	安全管理员

总则

为了保护学院的网络安全，防止学院的各种信息资产受到非授权访问，造成信息泄露，特制订本制度。

信息安全办公室主任负责监督网络管理员对有关网络安全工作的落实。

第一章 网络安全管理

1 帐号管理及认证授权

1.1 帐号

1）对登录网络设备的用户进行身份标识和鉴别，且用户的标识唯一，根据不同的使用人员分配不同的账号或账号组，修改系统默认的账号及口令，删除或锁定与设备运行和维护无关的账号。

2）根据不同的用户或角色分配不同的账号和账号组，避免不同角色之间共享账号。

3）限制超级账户直接远程登录并设置用户超时锁定策略。

1.2 口令

1）网络设备的登录口令应符合 3 种以上不同字符的复杂性要求、长度要求要 8 位以上、有效期要求为 90 天。

2）网络设备启用用户登录失败锁定功能，并限制 15 分钟失败登录次数为 3 次。

1.3 授权

应对登录网络设备的用户进行角色划分，根据用户的角色分配权限，实现用户的权限分离，仅授予用户所需的最小权限。

2 补丁管理

1) 每个季度进行一次采用专业的漏洞扫描、评估技术对网络设备进行定期安全评估，并根据结果对系统进行修复。
2) 每星期进行一次网络设备的补丁更新更新前必须进行补丁与现有业务系统的兼容性测试，确认后与系统提供厂商配合进行相应的修复。
3) 应对网络设备的漏洞发展情况进行跟踪，当出现新漏洞时，及时做好安全防护措施。

3 安全防护

1) 网络设备启用自身安全防护功能，防护对网络设备的攻击行为，保障自身设备的安全、稳定运行。
2) 重要网络设备采用 IP/MAC 绑定防止地址欺骗。

4 服务安全

1) 对进出网络的信息内容进行过滤，严格设置端口安全策略，关闭与系统运行无关端口；
2) 使用 SNMP 网络协议时，修改默认的 SNMP 团体字。
3) 禁止使用 Telnet 等存在安全隐患的协议。
4) 启用堡垒机，使用 SSH 协议管理。

5 安全审计

1) 网络设备启用日志审计功能，不仅包括对用户登录、用户操作进行记录，也要包括系统事件，安全事件等，日志应妥善保存、定期审计分析和备份，并确保日志记录的完整性。
2) 网络设备应配置远程日志功能，将重要日志内容传输到远程日志服务器。

6 安全管理

远程访问控制应满足下列的安全要求：

1) 通过设定终端接入方式、网络地址、端口范围等条件限制终端登录；
2) 严格限制匿名用户的访问权限；
3) 设置用户可以进行的最大连接数；
4) 网络设备远程管理过程中，应采用安全可靠的加密协议对通信过程中的整个报文或会话过程进行加密；
5) 对用户进行严格的访问控制，采用最小授权原则，分别授予不同用户各自为完成自己承担任务所需的最小权限；
6) 网络设备对连接超时进行限制，当用户登录设备后，5 分钟未进行操作后，就将自动中断此用户的连接。

7 备份恢复

1) 网络配置变更前后进行配置备份，如果网络配置没有变动则一周备份一次。每个月进行一次恢复性测试，以确保备份数据的可恢复性，并在《数据恢复申请表》中做相应记录。
2) 备份内容应定期转储存放到外部介质上（如磁带、光盘、服务器等），且上述外部介质应存放在值守保险柜中。

8 维护安全

1) 对所有运维网络设备的数据进行访问控制、授权、审批和审计并采取安全控制措施防止运维管理流量绕行审计系统。
2) 对网络设备进行监控，监控内容包括 CPU 使用率、硬盘使用率、内存、接口流量、系统事件、安全事件等信息。

9 废弃和重用

1) 网络设备废弃时，对废弃信息进行管理，主要包括数据备份、剩余信息清除和软硬件处理，并保存过程记录文档。
2) 网络设备重用前必须确保硬件上的数据被彻底删除。

10 日志管理

网络管理员每周要进行一次网络设备与安全设备日志收集分析，形成相应的日志分析报告，如果有异常上报信息安全办公室。

11 日常操作流程

网络设备与安全设备日常操作由网络管理员来执行,具体内容如下：

1) 检测设备内存是否异常；
2) 检测设备 CPU 是否异常；
3) 检测设备日志是否存在异常；
4) 检测设备的通信是否能正常使用；
5) 如有异常上报信息安全办公室。

第二章 网络结构及准入管理

1) 网络管理员根据实际网络，画出一份详细的网络拓扑图，并进行保存；在每次网络出现变动之后，对拓扑图进行更新，并以不同的版本号进行保存。
2) 网络管理员根据业务需求，对网络 IP 地址进行统一规划，统一分配和管理，并将人名、机器名进行绑定。
3) 系统内网严禁外来移动设备接入。

第三章 网络监控

1）须对机房网络设备的互联状况和设备本身运行情况进行监控，被监控对象出现异常时，监控系统发出报警。

2）由专门的运维监视平台接收并保存机房网络设备发送的日志及运行状态，并由值班人员查看服务器记录的日志信息。

3）网络管理员应妥善保管网络拓扑图、网络设备安全配置列表、设备规格及配置单、网络运行记录、网络检修记录等资料以备安全管理员检查。

4）网络管理员每个月对违反规定上网或其他违反网络安全策略的行为进行检查，并进行记录。