网络安全管理办法

(科应生所字〔2016〕85 号)

第一章 总则

第一条 为提高沈阳生态所处理突发信息网络事件的能力，形成科学、有效、反应迅速的应急工作机制，确保重要计算机信息系统的实体安全、运行安全和数据安全，最大限度地减少网络与信息安全突发公共事件的危害，保护公众利益，特制定本制度。

第二章 范围

第二条 本制度适用于沈阳生态所信息系统网络安全管理工作。

第三章 组织及职责

第三条 系统管理员职责

（一)恪守职业道德，严守企业秘密，熟悉国家安全生产法以及有关信息安全管理的相关规程；

（二）负责网络安全设备的安全策略部署、配置及变更管理、内网运行情况、更新和维护等日常工作；

（三）对数据网络实行分级授权管理，按照岗位职责授予不同的管理级别和权限；

（四）密切注意最新网络攻击行为的发生、发展情况，关注和追踪业界公布的攻击事件

（五）密切关注信息系统安全隐患，及时变更信息安全策略或升级安全设备。

第四条 信息安全管理员职责

（一)恪守职业道德，严守企业秘密，熟悉国家安全生产法以及有关信息安全管理的相关规程；

（二）每周对系统管理员的登录和操作记录进行审计；

（三）对系统管理员部署的安全策略、配置和变更内容进行审计；

（四）密切注意最新漏洞的发生、发展情况，关注和追踪业界公布的漏洞疫情。

第五条 管理员账号和权限管理

（一）管理员账号

系统管理员和信息安全管理员的用户账号应分开设置，其他人员不得设置账户。在安全设备上建立用户账号，需要经过本级信息部门安全主管的审批并保留审批记录。

（二）系统管理员权限

系统管理员具有设置、修改安全设备策略配置，以及读取和分析检测数据的权限。

（三）信息安全管理员权限

信息安全管理员具有读取安全设备日志信息，以及检查安全设备策略配置内容的权限。

（四）管理员身份鉴别

管理员身份鉴别可以采用口令方式。应为用户级和特权级模式设置口令，不能使用缺省口令，确保用户级和特权级模式口令不同。安全设备口令长度应采用 8 位以上，由非纯数字或字母组成，并保证每季度至少更换一次。

安全设备的身份鉴别，必要时可以采用数字证书方式。

第四章 策略和部署管理

第六条 制定安全策略

系统管理员应依据沈阳生态所管理系统信息安全规划，结合实际需求，制定、配置具体网络安全设备的安全策略，并且进行规范化和文档化；安全设备的策略文档应妥善保存。

对关键的安全设备要采用双机热备或冷备的方式进行部署以减小系统运行的风险。

第七条 安全设备统一部署

安全设备部署应依据沈阳生态所管理系统的信息安全规划统一部署，保证安全设备的可用性。安全设备部署的具体实施须经信息管理部门的审批并保留审批记录。

第八条 安全网关类设备部署

安全网关类设备部署应根据网络安全域的划分情况进行正确部署，满足不同网络安全域之间访问控制的要求。

第九条 入侵检测类设备部署

入侵检测类设备的部署要根据网络和信息系统的安全需求，选择合理的检测节点，能够完整的检测到被保护网络的数据流量，并能抓取含有足够信息的 IP 包，如：MAC 地址、IP 地址等。

第十条 漏洞扫描设备部署

漏洞扫描设备可采取离线或在线方式部署，部署前应进行漏洞扫描设备运行可能对系统影响的分析，避免对信息系统运行产生不良影响。

第五章 配置和变更管理

第十一条 配置和变更授权

网络安全设备的配置、变更应满足信息系统变更管理的要求，配置和变更前应充分评估对信息系统可能产生的影响，报信息管理部门审批、授权后执行，保留审批记录。

第十二条 防火墙设备配置

防火墙设备配置操作规程要点如下：记录网络环境，定义防火墙网络接口；定义防火墙的网络对象和应用端口；定义安全策略；定义系统管理员和信息安全管理员权限；测试防火墙性能；编写和整理防火墙设备配置文档和技术资料。

第十三条 VPN 设备配置

VPN 设备配置操作规程要点如下：

（一）环境配置，指网络环境的设置，VPN 网关的控制台的设置；

（二）设置 VPN 网关的各种网络参数特性，包括网络接口、透明网络、静态路由等；

（三）VPN 设置，将证书导入 VPN 网关系统；进行 SMC 设置，对 SMC 进行身份认证并下载策略，加载加密算法；添加静态隧道，从 SMC 中下载与本机有信任关系的主机信息；设置与信任设备之间的隧道各项参数，定义虚拟路由，并进行客户端配置；

（四）防火墙设置，包括进行包过滤规则设置和 NAT 规则设置；

（五）服务器设置，包括 VPN 安全网关提供的 DHCP 服务器、拨号服务器、L2tp 服务器、设置拨号用户、DNS 代理和 SNMP 代理等功能的话设置；

（六）带宽管理，对流经网络接口的网络流量预先进行分配管理，保证用户对网络连接带宽的要求。带宽管理针对所有网络接口进行管理；

（七）定义系统管理员和信息安全管理员权限；

（八）测试 VPN 安全网关性能；

（九）编写和整理 VPN 安全网关设备配置文档和技术资料。

第六章 代理服务器设备配置

第十四条 代理服务器设备配置操作规程要点如下：环境配置，指网络环境的设置，包括代理服务器对网络参数的设置；代理服务器安全策略设置；客户端的相关设置；定义系统管理员和信息安全管理员权限；性能参数测试，估测网络代理服务器吞吐量、延迟、并发连接数等；编写和整理代理服务器设备配置文档和技术资料。

第十五条 IP 加密机设备配置

IP 加密机设备配置操作规程要点如下：

（一）环境配置，指网络环境的设置，包括对密码机网络参数的设置；

（二）配置各加密机的安全策略；

（三）定义系统管理员和信息安全管理员权限；

（四）安全协议通用性测试，通过各种高层应用程序的测试，验证安全协议对高层应用的通用性；

（五）应用测试，包括网页浏览、文件传输、远程登录、邮件收发、视频播放；

（六）性能参数测试，估测加密机的吞吐率；

（七）编写和整理 IP 加密机设备配置文档和技术资料。

第十六条 入侵检测设备配置

入侵检测设备配置操作规程要点如下：

（一）记录当前网络环境，定义入侵检测接口；

（二）安装引擎（包括事件库）和管理软件；

（三）定义入侵检测系统要保护的网络对象（网络或主机）；

（四）定义检测策略，阻断级别和事件报警；

（五）定义系统管理员和信息安全管理员权限；

（六）编写和整理入侵检测设备配置文档和技术资料。

第十七条 漏洞扫描设备配置

漏洞扫描设备配置操作规程要点如下：

（一）记录网络环境，定义漏洞扫描的网络接口；

（二）定义漏洞扫描的 IP 地址范围；

（三）定义漏洞扫描的安全级别和扫描选项；

（四）安装、升级最新的漏洞库；

（五）定义系统管理员和信息安全管理员权限；

（六）编写和整理漏洞扫描设备配置文档和技术资料。

第七章 运行维护管理

第十八条 安全设备的检测和维护

安全网关及入侵检测类设备定期检测和维护要求如下：

（一）每月安装、更新厂家发布的设备补丁程序，及时修补设备操作系统的漏洞；

（二）每周审计一次日志报表；

（三）一个月内至少重新启动一次安全网关及入侵检测类设备。

第十九条 安全设备的监视和记录

安全网关及入侵检测类设备运行状况的监视和记录要求如下：

（一）系统管理员应定期和不定期地检查设备的运行状况，及时查看日志，对异常情况的发生，及时上报，并保存记录；

（二）对安全设备 CPU 和内存利用率、数据流量、地址翻译数量、报警次数等进行均时的监

测、跟踪工作，每周形成报表。

第二十条 安全设备配置备份和恢复

安全设备配置备份和恢复要求如下：

（一）定期备份安全设备配置；

（二）修改安全设备配置前应对现有配置进行备份，以便修改失败后可快速恢复；

（三）跟踪软件及事件库的变更，确保使用当前有效的软件及事件库。

第二十一条 安全设备的审计

信息安全管理员定期对网络安全设备的操作记录和内容本身进行审计，保证内容的完全性，保留记录。

第二十二条 安全事件处理和报告

防火墙设备发生宕机或入侵检测设备出现告警或工作不正常引起网络拥塞或网络瘫痪等安全事件时，系统管理员应立即启动紧急响应程序，保留相应记录。对网络进行紧急处理，堵塞攻击入口，恢复网络的正常运行，并追查攻击来源，及时上报，必要的情况下提交公安机关处理。

第二十三条 漏洞扫描设备的专项要求

（一）漏洞扫描设备工作时会对网络造成一定程度的影响，应避免在网络运行高峰期进行扫描，如有特殊情况应通知系统管理员；

（二）对扫描结果进行分析和对扫描出的安全漏洞进行修补；

（三）漏洞扫描设备定期检测和维护要求（首次实施）。系统管理员对服务器和专用网络设备实施首次漏洞扫描。服务器和专用网络设备上线前，必须进行漏洞扫描，并保留记录；

（四）漏洞扫描设备定期检测和维护要求（周期实施）。系统管理员对服务器和专用网络设备实施周期性漏洞扫描，并保留记录。

第二十四条 安全设备的维修

（一）安全设备的维修应防止安全设备配置信息的泄漏，送出外修应注意清除安全设备内部存储的安全配置；

（二）不允许厂商或服务商通过因特网或其它方式远程登录进行安全设备的维护；

（三）厂商或服务商进入现场维护安全设备，须指定专人全程陪同，维修完成后应进行安全检查。

第八章 安全数据管理

第二十五条 安全设备的数据

网络安全设备的安全数据主要包括安全设备对网络和系统检测得到的安全数据，对系统管理员操作的数据，对安全设备进行设置安全策略的配置数据，还有安全设备部署的网络逻辑图、安全策略等文档，应保证数据的完整性。

第二十六条 检测获得数据的管理

对于安全设备对网络和系统检测得到的安全数据，对系统管理员操作的数据，系统管理员和信息安全管理员应分别进行备份和保管；任何人不得进行修改，未经主管领导批准任何人不得删除。

系统管理员定期分析安全设备对网络和系统检测得到的安全数据，发现漏洞或隐患应及时报告，并形成分析报告。

第二十七条 获得数据的管理

信息安全管理员应定期分析安全设备对系统管理员操作的数据，发现违规问题或隐患应及时报告，并形成分析报告。

第二十八条 配置数据管理

系统管理员应及时对安全设备进行设置安全策略（规则）的配置数据进行备份和保存，对安全设备部署的网络逻辑图、安全策略等文档也应进行妥善保管。

第二十九条 存储空间管理

系统管理员应经常检查安全设备的存储空间，注意防止安全设备中对网络和系统检测得到的安全数据，以及对系统管理员操作的数据的丢失。

第三十条 设备选型管理

网络安全设备（产品）的使用应符合国家的有关规定，尽量采用具有计算机信息系统安全专用产品销售许可证的信息安全产品，且具有中国信息安全产品测评认证中心认证的信息安全产品。

密码设备选型应符合国家密码主管部门的有关要求，加密算法应得到国家密码主管部门的批准。

第九章 使用国际互联网的规定

第三十一条 管理系统与互联网实行严格的物理隔离，严禁用处理管理系统秘密信息的计算机上互联网，违者严肃查处。

第三十二条 采取切实措施，加强对计算机的使用管理，上互联网的计算机必须与处理管理系统秘密信息的计算机严格区分，做到专机专用，不得既用于上互联网又用于处理国家秘密信息。

第三十三条 使用物理隔离计算机一机两用的，物理隔离计算机必须采用经国家保密局批准的产品，使用中应严格规范操作，严防由于误操作造成泄密。在目前尚不能确保安全的情况下，禁止任何单位将网络安全隔离与交换设备（又称网闸）用于涉密信息网络和互联网之间。

第三十四条 加强计算机及网络安全保密知识教育，加强保密形势教育，使涉密人员懂得用涉密计算机上互联网的严重危害性，提高信息安全保密意识，自觉遵守保密纪律和有关保密规定。

第三十五条 切实加强对计算机及网络的保密管理，建立健全规章制度，并严格执行；加强保密技术检查，及时发现违反规定的行为，堵塞泄密漏洞。

第三十六条 凡计算机使用人要按照《沈阳生态所计算机信息系统安全保密管理制度》的规定操作计算机。

第三十七条 经常对涉密计算机和涉密网络的保密管理情况进行检查，如发现问题，应立即整改纠正；问题严重并造成一定影响或损失的，要追究相关人员的责任。

第十章 附则

第三十八条 本办法由信息中心负责解释。

第三十九条 本办法自印发之日起执行。