

附件 2

网络安全管理工作自评估表

(注：蓝色--自主采取措施解决；红色--需要外部技术服务或产品解决；)

评估指标	评价要素	评价标准	权重 (V)	指标属性	量化方法 (P 为量化值)	评估得分 (V×P)
网络安全组织管理	网络安全主管领导	明确一名主管领导负责本部门网络安全工作 (主管领导应为本部门正职或副职领导)。	3	定性	已明确, 本年度就网络安全工作作出批示或主持召开专题会议, P=1; 已明确, 本年度未就网络安全工作作出批示或主持召开专题会议, P=0.5; 尚未明确, P=0。	
	网络安全管理机构	指定一个机构具体承担网络安全管理工作 (管理机构应为本部门二级机构)。	2	定性	已指定, 并以正式文件等形式明确其职责, P=1; 未指定, P=0。	
	网络安全员	各内设机构指定一名专职或兼职网络安全员。	2	定量	P = 指定网络安全员的内设机构数量与内设机构总数的比率。	
网络安全日常管理	规章制度	制度完整性	3	定性	制度完整, P=1; 制度不完整, P=0.5; 无制度, P=0。	
		制度发布	2	定性	符合, P=1; 不符合, P=0。	
	人员管理	重点岗位人员签订安全保密协议	2	定量	P = 重点岗位人员中签订网络安全与保密协议的比率。	

评估指标		评价要素	评价标准	权重 (V)	指标 属性	量化方法 (P 为量化值)	评估得分 (V×P)
		人员离岗离职管理措施	人员离岗离职时, 收回其相关权限, 签署安全保密承诺书。	2	定性	符合, P = 1; 不符合, P = 0。	
		外部人员访问管理措施	外部人员访问机房等重要区域时采取审批、人员陪同、进出记录等安全管理措施。	2	定性	符合, P = 1; 不符合, P = 0。	
	资产管理	责任落实	指定专人负责资产管理, 并明确责任人职责。	2	定性	符合, P = 1; 不符合, P = 0。	
		建立台账	建立完整资产台账, 统一编号、统一标识、统一发放。	2	定性	符合, P = 1; 不符合, P = 0。	
		账物符合度	资产台账与实际设备相一致。	2	定性	符合, P = 1; 不符合, P = 0。	
		设备维修维护和报废管理措施	完整记录设备维修维护和报废信息(时间、地点、内容、责任人等)。	2	定性	记录完整, P = 1; 记录基本完整, P = 0.5; 记录不完整或无记录, P = 0。	
	外包管理	外包服务协议	与信息技术外包服务提供商签订网络安全与保密协议, 或在服务合同中明确信息安全与保密责任。	2	定性	符合, P = 1; 不符合, P = 0。	
		现场服务管理	现场服务过程中安排专人管理, 并记录服务过程。	2	定性	记录完整, P = 1; 记录不完整, P = 0.5; 无记录, P = 0。	
		外包开发管理	外包开发的系统、软件上线前通过信息安全测评。	2	定量	P = 外包开发的系统、软件上线前通过信息安全测评的比率。	
		运维服务方式	原则上不得采用远程在线方式, 确需采用时采取书面审批、访问控制、在线监测、日志审计等安全防护措施。	2	定性	符合, P = 1; 不符合, P = 0。	
	经费保障	经费预算	将网络安全设施运维、日常管理、教育培训、检查评估等费用纳入年度预算。	3	定性	符合, P = 1; 不符合, P = 0。	

评估指标		评价要素	评价标准	权重 (V)	指标属性	量化方法 (P 为量化值)	评估得分 (V×P)
	网站内容管理	网站信息发布	网站信息发布前采取内容核查、审批等安全管理措施。	2	定性	符合, P = 1; 不符合, P = 0。	
	电子信息管理	介质销毁和信息消除	配备必要的电子信息消除和销毁设备, 对变更用途的存储介质进行信息消除, 对废弃的存储介质进行销毁。	1	定性	符合, P = 1; 不符合, P = 0。	
信息安全防护管理	物理环境安全	机房安全	具备防盗窃、防破坏、防雷击、防火、防水、防潮、防静电及备用电力供应、温湿度控制、电磁防护等安全措施。	2	定性	符合, P = 1; 不符合, P = 0。	
		物理访问控制	机房配备门禁系统或有专人值守。	1	定性	符合, P = 1; 不符合, P = 0。	
	网络边界安全	访问控制	网络边界部署访问控制设备, 能够阻断非授权访问。	3	定性	符合, P = 1; 有设备, 但未配置策略, P = 0.5; 无设备, P = 0。	
		入侵检测	网络边界部署入侵检测设备, 定期更新检测规则库。	2	定性	符合, P = 1; 有设备, 但未定期更新, P = 0.5; 无设备, P = 0。	
		安全审计	网络边界部署安全审计设备, 对网络访问情况进行定期分析审计并记录审计情况。	2	定性	符合, P = 1; 有设备, 但未定期分析, P = 0.5; 无设备, P = 0。	
		互联网接入口数量	各单位同一办公区域内互联网接入口不超过 2 个。	2	定性	符合, P = 1; 不符合, P = 0。	
	设备安全	恶意代码防护	部署防病毒网关或统一安装防病毒软件, 并定期更新恶意代码库。	2	定性	符合, P = 1; 有设备, 但未定期更新, P=0.5 无设备, P = 0。	
		设备漏洞扫描	定期对服务器、网络设备、安全等进行安全漏洞扫描。	2	定性	符合, P = 1; 不符合, P = 0。	

评估指标		评价要素	评价标准	权重 (V)	指标属性	量化方法 (P 为量化值)	评估得分 (V×P)
		服务器口令策略	配置口令策略保证服务器口令强度和更新频率。	1	定量	P = 配置了口令策略的服务器比率。	
		服务器安全审计	启用安全审计功能并进行定期分析。	1	定量	P = 对安全审计日志进行定期分析的服务器比率。	
		服务器补丁更新	及时对服务器操作系统补丁和数据库管理系统补丁进行更新。	2	定量	P = 补丁得到及时更新的服务器比率。	
		网络设备和安全设备口令策略	配置口令策略保证网络设备和安全设备口令强度和更新频率。	1	定量	P = 网络设备和安全设备（指重要设备）中配置了口令策略的比率。	
		终端计算机统一防护	采取集中统一管理方式对终端进行防护，统一软件下载、安装系统补丁。	2	定性	符合，P = 1； 不符合，P = 0。	
		终端计算机接入控制	采取技术措施（如部署集中管理系统、将 IP 地址与 MAC 地址绑定等）对接入本单位网络的终端计算机进行控制。	1	定性	符合，P = 1； 不符合，P = 0。	
	应用系统安全	应用系统安全漏洞扫描	定期对服务器、网络设备、安全设备等进行安全漏洞扫描。	2	定性	扫描周期小于 1 个月，P=1； 扫描周期为 2 到 3 个月，P=0.5 扫描周期为 4 到 6 个月，P=0.2 其他，P=0。	
		门户网站防篡改措施	门户网站采取网页防篡改措施。	2	定性	符合，P = 1； 不符合，P = 0。	
		门户网站抗拒绝服务攻击措施	门户网站采取抗拒绝服务攻击措施。	1	定性	符合，P = 1； 不符合，P = 0。	
		电子邮件账号注册审批	建立邮件账号开通审批程序，防止邮件账号任意注册使用。	1	定性	符合，P = 1； 不符合，P = 0。	

评估指标		评价要素	评价标准	权重 (V)	指标 属性	量化方法 (P 为量化值)	评估得分 (V×P)
数据安全	电子邮箱账户口令策略	电子邮箱账户口令策略	配置口令策略保证电子邮箱口令强度和更新频率。	1	定性	符合, P = 1; 不符合, P = 0。	
		邮件清理	定期清理工作邮件。	1	定性	符合, P = 1; 不符合, P = 0。	
	数据存储保护	数据存储保护	采取技术措施 (如加密、分区存储等) 对存储的重要数据进行保护。	2	定性	符合, P = 1; 不符合, P = 0。	
		数据传输保护	采取技术措施对传输的重要数据进行加密和校验。	2	定性	符合, P = 1; 不符合, P = 0。	
		数据和系统备份	采取技术措施对重要数据和系统进行定期备份。	2	定性	符合, P = 1; 不符合, P = 0。	
		数据中心、灾备中心设立	数据中心、灾备中心应设立在境内。	1	定性	符合, P = 1; 不符合, P = 0。	
网络安全应急管理	应急预案	制定网络安全事件应急预案 (为部门级预案, 非单个信息系统的安全应急预案), 并使相关人员熟悉应急预案。	2	定性	符合, P = 1; 不符合, P = 0。		
	应急演练	开展应急演练, 并留存演练计划、方案、记录、总结等文档。	2	定性	符合, P = 1; 不符合, P = 0。		
	应急资源	指定应急技术支援队伍, 配备必要的备机、备件等应急物资。	1	定性	符合, P = 1; 不符合, P = 0。		
	事件处置	发生网络安全事件后, 及时向主管领导报告, 按照预案开展处置工作; 重大事件及时通报网络安全主管部门。	2	定性	发生过事件并按要求处置, 或者未发生过安全事件, P = 1; 发生过事件但未按要求处置, P = 0。		
网络安全教育培训	意识教育	面向全体人员开展网络安全形势与警示教育、基本技能培训等活动。	3	定量	本年度开展活动的次数 ≥ 3, P = 1; 次数=2, P = 0.7; 次数=1, P = 0.3; 次数=0, P = 0。		

评估指标	评价要素	评价标准	权重 (V)	指标 属性	量化方法 (P 为量化值)	评估得分 (V×P)
	专业培训	定期开展网络安全管理和技术人员专业培训。	3	定量	P = 本年度网络安全管理和技术人员中参加专业培训的比率。	
网络安全检查	工作部署	下发检查工作相关文件或者组织召开专题会议，对年度检查工作进行部署。	2	定性	符合，P = 1； 不符合，P = 0。	
	工作机制	明确检查工作负责人，落实检查机构和检查人员。	2	定性	符合，P = 1； 不符合，P = 0。	
	技术检测	使用技术手段进行安全检测	2	定性	符合，P = 1； 不符合，P = 0。	
	检查经费	安排并落实检查工作经费。	2	定性	符合，P = 1； 不符合，P = 0。	