网络与信息安全管理师

职业能力等级评价标准

（试行稿）

1 项目概况

1.1 项目名称

网络与信息安全管理师

1.2 项目定义

从事网络及信息安全管理、防护、监控工作的人员。

1.3 能力等级

本项目共设三个等级，分别为：初级、中级、高级。

1.4 能力特征

（1）具有一定的组织、理解、判断能力，具有较强的学习能力、分析解决问题的能力和沟通能力。

（2）具有扎实的计算机基础知识、网络通信、软件开发等相关学科的基本知识。

（3）能够阅读英文的专业科技文献，不仅具备运用英语进行沟通和交流的能力，而且具备运用计算机及信息网络辅助信息安全系统规划、设计、计算、控制的能力，有获取最新科学技术知识和信息的能力。

1.5 职业能力等级评价要求

1.5.1 申报条件

具备以下条件之一者，可申报初级：

（1）累计从事相关职业工作1年（含）以上。

（2）相关专业在校学生。

具备以下条件之一者，可申报中级：

（1）取得本项目或相关职业初级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作2年（含）以上。

（2）累计从事相关职业工作4年（含）以上。

（3）取得相关专业毕业证书。

具备以下条件之一者，可申报高级：

（1）取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作3年（含）以上。

（2）累计从事相关职业工作6年（含）以上。

（3）具有高等职业学校、高级技工学校、技师学院相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）。

（4）具有大专及以上相关专业毕业证书，并取得本项目或相关职业中级评价证书（含职业资格证书、职业技能等级证书等）后，累计从事相关职业工作1年（含）以上。

1.5.2 申报条件注释

（1）满足本项目高级别申报条件可申报本项目低级别。

（2）相关职业：应用电子、信息通信类等职业。

（3）相关专业：电子信息类专业6101；

计算机类专业6102；

通信类专业6103。

1.5.3 评价方式

职业能力等级评价考试包括理论知识、技能操作两个科目，较高等级必要时可增加综合评审。

理论知识考试以笔试为主，可以机考，条件成熟时试点开展网络考试，主要考核从业人员从事本职业应掌握的基本要求和相关知识要求。技能操作考核主要采用现场操作、模拟操作、面试答辩等方式进行，主要考核从业人员从事本职业应具备的技能水平。综合评审通常采取审阅申报材料、技术答辩等方式进行全面评议和审查。理论知识考试和技能操作考核均采用百分制，成绩达到60分以上者为合格。

1.5.4 监考人员、考评人员与考生配比

理论知识考试监考人员与考生配比为1:20，每个标准教室配备监考人员不少于2名；技能操作考核考评员与考生配比为1:4～1:6，且不少于3名考评员。

1.5.5 评价时间

各等级理论知识考试时间不少于90分钟；各等级技能操作考核时间为90～120分钟。

1.5.6 评价场所设备

理论知识考试在标准教室内进行；技能操作考核根据各模块的工作要求，在配备有通信及网络信息安全相关硬件、软件，且能进行网络通信安全操作及安全配置的场所。

2 基本要求

2.1 职业道德

（1）爱岗敬业，恪尽职守。

（2）精通技术，保证质量。

（3）遵纪守法，严守秘密。

（4）文明生产，热情服务。

2.2 基础知识

2.2.1 通用基础知识

（1）计算机组成。

（2）操作系统知识。

（3）数据库知识。

（4）中间件知识。

（5）计算机应用软件知识。

（6）计算机网络知识。

（7）虚拟化技术知识。

2.2.2 网络安全基础知识

（1）网络安全保障知识。

（2）互联网物理与网络通信安全技术知识。

（3）密码技术知识。

（4）恶意代码与防护知识。

（5）渗透测试与安全漏洞知识。

（6）安全运维知识。

（7）网络安全管理体系知识。

2.2.3 法律法规知识

（1）法律（详见附录一）

《宪法》第40条

《刑法》第124条

《中华人民共和国国家安全法》

《中华人民共和国网络安全法》

《中华人民共和国保守国家秘密法》

《中华人民共和国反恐怖主义法》

（2）行政法规

《中华人民共和国电信条例》

《国家网络安全事件应急预案》

（3）行政规章

《电信服务规范》

《公用电信网间互联管理规定》

《电信设备进网管理办法》

《电信业务经营许可管理办法》

《通信网络安全防护管理办法》

《电信和互联网用户个人信息保护规定》

《电信网和互联网管理安全等级保护要求》

《关键信息基础设施安全保护条例》

《计算机信息网络国际互联网安全保护管理办法》

（4）国家、相关主管部门及地方政府和主管部门颁布的其他有关网络与信息安全管理的法律法规及行政规章

3 工作要求

本标准对初级、中级、高级各级别的技能要求依次递进，高级别涵盖低级别的要求。

3.1 初级

职业功能	工作内容	技能要求	相关知识
1.安全事件的监测处置与检测评估	1.1 安全事件的监测与发现	1.1.1 能够查看并识别操作系统实时运行状态 1.1.2 能够识别系统/设备安全事件的告警信息，并能分析登陆、配置等系统安全事件日志 1.1.3 能够按照应急处置流程，记录并上报网络安全事件 1.1.4 能够识别暴力破解、缓冲区溢出等终端类攻击手段及其特征 1.1.5 能够利用扫描工具，检测发现系统漏洞	1.1.1 操作系统的日志/告警原理 1.1.2 网络设备、安全设备的日志/告警原理 1.1.3 网络安全事件应急处置流程 1.1.4 缓冲区溢出漏洞原理 1.1.5 系统漏洞扫描软件使用方法
	1.2 安全事件的应对与处理	1.2.1 能够识别病毒感染、木马植入等终端类攻击事件 1.2.2 能够从WEB日志中分析SQL注入、XSS等WEB类网络攻击事件 1.2.3 能够查看并识别操作系统中的运行进程，并能够清理其中的恶意进程 1.2.4 能够对木马、僵尸、蠕虫类终端安全事件进行处置	1.2.1 病毒感染、木马植入等终端类攻击事件的识别方法 1.2.2 WEB日志的分析方法 1.2.3 操作系统恶意进程检测及清理方法 1.2.4 恶意程序类攻击事件的处置方法
	1.3 安全事件的检测与评估	1.3.1 能够通过资产识别、人员访谈等，进行符合性评测 1.3.2 能够实施SSH、TELNET、WEB等应用的弱口令检测 1.3.3 能够使用NMAP等探测性扫描软件，进行端口扫描、应用识别等检测工作 1.3.4 能够使用系统漏洞扫描工具，发现版本漏洞、弱口令等系统漏洞	1.3.1 符合性评估工作方法 1.3.2 弱口令检测方法 1.3.3 端口/应用扫描方法 1.3.4 安全漏洞扫描方法

2.系统的策略配置与安全加固	2.1 操作系统安全配置	2.1.1 能够安装操作系统并完成初始化配置 2.1.2 能够识别资源管理、网络通信等操作系统应用进程 2.1.3 能够配置并管理网络操作系统的注册表 2.1.4 能够实施网络操作系统的用户管理 2.1.5 能够完成操作系统中输入法、驱动程序、文件夹等自启动项管理操作 2.1.6 能够实施并管理操作系统中的文件共享 2.1.7 能够完成操作系统中用户与口令管理，并能发现异常用户信息 2.1.8 能够识别操作系统中异常的进程与线程	2.1.1 操作系统安装方法 2.1.2 操作系统进程识别技术知识 2.1.3 注册表、用户管理类命令的使用方法 2.1.4 操作系统自启动项管理方法 2.1.5 操作系统文件共享管理方法 2.1.6 操作系统用户管理方法 2.1.7 操作系统异常进程与线程的判别方法
	2.2 数据库安全配置	2.2.1 能够完成MYSQL、SQL SERVER数据库的安装与初始化配置 2.2.2 能够使用数据库管理软件，完成数据库查询、插入、删除、备份等操作 2.2.3 能够识别并使用数据库应用/编程接口 2.2.4 能够实施数据库用户增加、注销等用户组权限分配与管理操作	2.2.1 数据库安装方法 2.2.2 数据库管理软件使用方法 2.2.3 数据库系统应用/编程接口调用方法 2.2.4 数据库用户管理方法
	2.3 网络安全产品配置	2.3.1 能够识别交换机、路由器、防火墙、WAF等网络安全产品的应用场景与业务功能 2.3.2 能够配置交换机、路由器、防火墙、WAF等网络安全产品 2.3.3 能够在企业级网络系统内，设计多个安全产品的部署方案 2.3.4 能够完成用户添加、权限	2.3.1 交换机、路由器的配置方法 2.3.2 防火墙产品的配置方法 2.3.3 WAF产品的配置方法 2.3.4 网络安全产品的用户权限管理方法 2.3.5 路由器包过滤配置方法

		控制等网络安全产品账号权限的分配和管理操作 2.3.5 能够配置路由器，实现IP过滤、端口过滤等包过滤规则	
	2.4 WEB服务器的安全配置	2.4.1 能够分配并管理WEB服务器的用户组权限 2.4.2 能够配置WEB服务的访问控制策略 2.4.3 能够识别SQL注入、XSS、文件上传等WEB攻击 2.4.4 能够实施域名、IP、上传包类型等WEB服务访问限制策略的配置操作 2.4.5 能够完成IIS、Apache等WEB服务器中间件与发布程序的安装	2.4.1 WEB服务器用户权限管理方法 2.4.2 WEB服务访问控制管理方法 2.4.3 WEB攻击识别方法 2.4.4 WEB服务访问控制原理 2.4.5 WEB中间件安装管理方法
3.互联网信息安全与网络环境治理	3.1 信息安全基础管理	3.1.1 能够完成网站备案真实性核验工作 3.1.2 能依据IP地址报备的流程和要求，根据IP地址的不同应用场景，对IP地址进行分类报备 3.1.3 能够对未备案网站、备案信息不准确等情况进行处置 3.1.4 能够对各类IP报备异常情况进行处置	3.1.1 网站备案真实性核验工作流程和要求 3.1.2 IP网络资源管理知识 3.1.3 网站备案工作流程和要求 3.1.4 ICP/IP网站工作流程和要求 3.1.5 IP备案管理知识
	3.2 信息安全系统管理	3.2.1 能够按IDC信息安全管理系统规范要求填报各类数据 3.2.2 能够根据ICP/IP备案系统的不同条件检索各类数据 3.2.3 能够处理上级IDC系统下发的数据 3.2.4 能够完成IDC系统评测相关工作	3.2.1 IDC/ISP信息安全管理系统基本管理要求 3.2.2 IDC系统评测要求 3.2.3 网站备案和IP地址报备（ICP/IP）系统使用规范 3.2.4 IDC/ISP信息安全管理系统技术要求 3.2.5 网站备案和IP地址报备（ICP/IP）系统技术要求
	3.3 网络环境信息治理	3.3.1 能够识别并处理互联网各类违法违规行为 3.3.2 能够判别并处置端口类和点对点垃圾短信	3.3.1 互联网“九不准”等违法违规行为的内容 3.3.2 垃圾短信发现和处置策略配置方法

		3.3.3 能够对互联网新技术新业务进行分类 3.3.4 能够对互联网上各类不良信息及垃圾短信进行监测和处置，并检测发现新型垃圾短信 3.3.5 能够开展新用户实名登记和老用户补登记的办理工作 3.3.6 能够对互联网新技术新业务进行分类并分析判断其存在的信息安全风险，开展预评估	3.3.3 互联网新技术新业务分类标准 3.3.4 互联网和通信短信息不良信息的处置方法 3.3.5 电话用户实名制工作要求 3.3.6 互联网新技术新业务信息安全评估指南和相关工作要求

3.2 中级

职业功能	工作内容	技能要求	相关知识
1.安全事件的监测处置与检测评估	1.1 安全事件的监测与发现	1.1.1 能够识别权限绕过、文件上传等WEB类攻击手段及其特征 1.1.2 能够识别编码过程中的不规范行为 1.1.3 能够通过代码审计，识别应用中存在的SQL注入、XSS等漏洞 1.1.4 能通过数据报文抓取、分析，在网络层面识别内网的安全事件 1.1.5 能识别逻辑漏洞类、WEB类攻击手段及其网络通信特征，并提出修改策略	1.1.1 WEB权限绕过攻击识别方法 1.1.2 代码审计与漏洞挖掘技术知识 1.1.3 内网渗透及防护知识 1.1.4 数据报文抓取和分析方法
	1.2 安全事件的应对与处理	1.2.1 能够对源代码缺陷类WEB网络安全事件进行处置 1.2.2 能够对WEBSHELL、反弹木马等WEB恶意代码进行识别并清除 1.2.3 能够应用逆向反汇编技术，识别后门类恶意软件 1.2.4 能够运用数据恢复技术，对网络攻击行为进行取证 1.2.5 能够组织、实施针对大规模流量攻击的应急处置	1.2.1 源代码级WEB类漏洞处置方法 1.2.2 WEB类后门类恶意程序识别方法 1.2.3 逆向反汇编技术知识 1.2.4 计算机取证技术知识 1.2.5 数据恢复技术知识 1.2.6 大规模流量攻击的处置方法
	1.3 安全事件的检测与评估	1.3.1 能够完成WEB渗透测试工作 1.3.2 能够完成终端类渗透测试工作	1.3.1 WEB渗透测试技术方法 1.3.2 终端渗透测试技术方法 1.3.3 符合性评估与安全审计

		1.3.3 能够开展风险识别、访问控制等安全审计工作 1.3.4 能够从业务影响、恢复策略等方面实施业务连贯性评估 1.3.5 能够参照检测/评估标准，使用多种检测方法，组织实施企业级业务系统的检测评估	工作原理 1.3.4 业务连贯性评估方法 1.3.5 网络系统安全检测/评估标准
2.系统的策略配置与安全加固	2.1 操作系统安全配置	2.1.1 能够对操作系统进行访问控制策略配置 2.1.2 能够针对操作系统，完成NTP、FTP、SSH等常见的服务配置与管理操作	2.1.1 操作系统访问控制策略实施方法 2.1.2 操作系统应用服务的配置与管理方法
	2.2 数据库安全配置	2.2.1 能够实施数据库表、视图等资源的访问控制操作 2.2.2 能够实施数据库应用接口、实例等服务配置与服务管理 2.2.3 能够实施数据完整性核验、数据恢复、数据备份等数据管理类操作 2.2.4 能够实施数据库查询、插入、删除备份等操作类指令的行为审计 2.2.5 能够识别并处置数据库SQL注入、文件DUMP等常见的攻击手段	2.2.1 数据库访问控制方法 2.2.2 数据库应用接口与服务管理方法 2.2.3 数据库系统数据完整性核验/数据备份和恢复方法 2.2.4 数据库系统行为审计方法 2.2.5 数据库系统渗透方法
	2.3 网络安全产品配置	2.3.1 能够配置安全隔离网闸，实现敏感网络与公共网络的数据传输 2.3.2 能够配置VPN设备，实现专用网络的配置与部署 2.3.3 能够配置入侵检测设备（IDS），完成恶意程序、WEB渗透等攻击的识别	2.3.1 安全隔离网闸设备的配置方法 2.3.2 VPN技术原理及设备配置方法 2.3.3 入侵检测设备技术原理及配置方法
	2.4 WEB 服务器的安全配置	2.4.1 能够使用WEB安全扫描及渗透工具，对网站漏洞进行检测 2.4.2 能够实施日志挖掘、可疑文件排查等操作，完成WEB安全威胁分析与处置操作 2.4.3 能够实施针对大规模流量攻击的安全防护操作	2.4.1 WEB安全扫描与渗透技术方法 2.4.2 WEB日志分析方法 2.4.3 WEB大规模流量攻击的处置方法 2.4.4 WEB服务器的配置与管理方法

		2.4.4 能够完成WEB服务器中间件与发布程序的配置与管理 2.4.5 能够对SQL注入、XSS、文件上传等WEB漏洞实施源代码级的安全加固 2.4.6 能够进行脚本语言开发，实现WEB安全基线、异常文件、日志的检查，编制系统风险报告	2.4.5 WEB漏洞的源代码级加固方法 2.4.6 脚本语言编程方法 2.4.7 WEB中间件及发布程序的配置与管理方法
3.互联网信息安全与网络环境治理	3.1 信息安全基础管理	3.1.1 能够完整开展网站备案和IP地址新增、变更、删除等操作 3.1.2 能够通过设计技术方案，主动发现未备案网站和备案信息不准确等异常情况 3.1.3 能够通过设计技术方案主动发现各类IP异常情况并报备	3.1.1 信息安全业务处理流程 3.1.2 互联网网络框架知识
	3.2 信息安全系统管理	3.2.1 能够判断并处理ICP/IP备案系统异常数据 3.2.2 能够对IDC系统接口、数据交互和存储等进行管理维护并能够组织实施IDC系统评测 3.2.3 能够对ICP/IP备案系统接口、数据交互和存储等进行管理维护	3.2.1 网站备案和IP地址报备（ICP/IP）系统技术要求 3.2.2 IDC/ISP信息安全管理系统接口规范 3.2.3 IDC系统评测技术要求及组织管理办法 3.2.4 网站备案和IP地址报备（ICP/IP）系统接口规范
	3.3 网络环境信息治理	3.3.1 能发现并处理上级下发的各类信息安全事件 3.3.2 能够对各类垃圾短信数据进行综合大数据分析 3.3.3 能够判断并处置用户登记违规、违规网络改号各类实名制违规问题 3.3.4 能够独立完成新技术新业务评 估报告	3.3.1 互联网管理基本框架结构 3.3.2 大数据基础知识 3.3.3 号码传送规范 3.3.4 网络与信息安全前瞻性新技术新业务评估知识 3.3.5 互联网新技术新业务信息安全评估指南和相关工作要求
4.培训指导	4.1 培训	4.1.1 能够组织培训技术人员，实施操作系统的安装、配置、加固与应急处置 4.1.2 能对技术人员实施网络安全设备配置进行培训	4.1.1 培训规范与流程

	4.2 指导	4.2.1 能够指导初级技术人员完成网络安全事件应对处置 4.2.2 能够指导初级技术人员完成WEB应用的安全加固与应对处置	4.2.1 网络安全事件应对流程与处置技巧 4.2.2 实施WEB应用安全加固与应急处置的知识

3.3 高级

职业功能	工作内容	技能要求	相关知识
1.安全事件的监测处置与检测评估	1.1安全事件的监测与发现	1.1.1 能够在移动终端操作系统中识别移动网络安全攻击事件 1.1.2 能够在大规模系统中，运用大数据、云计算等技术，分析预警网络安全风险 1.1.3 能够编制并设计重要信息系统网络安全防护监测体系	1.1.1 移动互联网安全知识 1.1.2 工业控制系统安全知识 1.1.3 云计算安全防护与虚拟化知识 1.1.4 物联网安全知识 1.1.5 区块链安全知识 1.1.6 大数据安全知识 1.1.7 人工智能安全知识 1.1.8 网络安全风险评估方法
	1.2安全事件的应对与处理	1.2.1 能够设计并组织实施针对重要信息系统的网络安全防护方案 1.2.2 能够针对系统脆弱性，结合已有技术手段，设计并组织实施网络安全应急演练 1.2.3 能够针对系统面临的安全风险，设计应急响应方案，进行攻击事件处置能力的顶层设计	1.2.1 网络安全攻防对抗知识 1.2.2 应急演练的设计方法 1.2.3 应急响应方案的设计方法
	1.3安全事件的检测与评估	1.3.1 能够运用社会工程学、模糊测试等手段优化安全检测流程，分析识别系统的安全风险点 1.3.2 能够设计并维护网络安全检测/评估过程中的工具集，实施稳定、可控、标准的安全检测工作 1.3.3 能够设计并编制系统风险评估报告，实现系统面临威胁、存在弱点、造成影响的量化评估	1.3.1 社会工程学检测方法 1.3.2 模糊测试方法 1.3.3 检测/评估报告的编制方法
2.系统的策略配置与安全加固	2.1操作系统安全配置	2.1.1 能够分析、验证操作系统漏洞，跟踪操作系统最新高危漏洞动态 2.1.2 能够识别操作系统安全威胁，分析操作系统脆弱性	2.1.1 操作系统漏洞原理 2.1.2 操作系统威胁识别原理 2.1.3 操作系统安全体系结构和设计原理

职业功能	工作内容	技能要求	相关知识
		2.1.3 能够针对系统业务特点，制定系统内各类操作系统的安全配置标准 完成操作系统防护能力的设计 2.1.4 能完成操作系统加固	
	2.2数据库安全配置	2.2.1 能够分析、验证数据库漏洞，跟踪数据库最新高危漏洞动态 2.2.2 能够设计并组织实施数据库异地备份/容灾备份 2.2.3 能够针对系统特点，制定系统内各版本数据库的安全配置标准，完成数据库系统防护能力的设计	2.2.1 数据库系统应用漏洞检测技术 2.2.2 数据库容灾备份技术 2.2.3 数据库安全体系结构和设计方法
	2.3网络安全产品配置	2.3.1 能够在城域网级别，完成安全产品部署方案的规划与设计 2.3.2 能够分析各类网络安全产品所产生的告警/日志数据，挖掘系统面临的安全威胁	2.3.1 系统安全模型设计方法 2.3.2 运行安全模式评估方法 2.3.3 网络安全产品日志数据分析方法
	2.4WEB 服务器的安全配置	2.4.1 能够对WEB系统/应用程序进行源代码级分析，并能够编制风险预警方案 2.4.2 能够分析、验证WEB应用程序漏洞，跟踪WEB最新高危漏洞动态	2.4.1 WEB源代码审计方法 2.4.2 WEB安全漏洞原理
3.互联网信息安全与网络环境治理	3.1信息安全基础管理	3.1.1 能够指导工作人员开展网站备案工作 3.1.2 能够对网站备案数据进行综合数据分析并给出分析报告 3.1.3 能够指导工作人员开展IP地址报备工作 3.1.4 能够对IP地址报备等数据进行综合数据分析并给出分析报告	3.1.1 数据处理方法 3.1.2 报表制作规范 3.1.3 数据分析与展现 3.1.4 专业报告规范
	3.2信息安全系统管理	3.2.1 能按照IDC信息安全管理系统技术要求和接口规范，根据企业情况制定企业侧系统建设方案 3.2.2 能够针对ICP/IP备案系统的功能和数据资源，制定数据分析和	3.2.1 系统建设管理知识 3.2.2 项目管理知识

职业功能	工作内容	技能要求	相关知识
		系统优化方案，解决或改善未备案网站和备案数据异常等问题	
	3.3网络环境信息治理	3.3.1 能够设计信息安全应急演练方案，并组织实施信息安全应急演练 3.3.2 能够根据企业自身情况，制定垃圾短信发现和处置方案 3.3.3 能够设计实名制工作检查方案并组织开展现场检查核验 3.3.4 能够制定企业内部新技术新业务评估方案，建立互联网新技术新业务信息安全评估工作机制 3.3.5 能够组织开展互联网新技术信息安全评估培训	3.3.1 信息安全事件应急处置策略 3.3.2 主流厂家的最新设备性能和组网方案 3.3.3 网络与信息安全主要标准知识 3.3.4 网络与信息安全产品的部署与选型应用知识 3.3.5 网络与信息安全解决方案编写知识 3.3.6 网络与信息安全前瞻性新技术评估培训知识
4.培训指导	4.1培训	4.1.1 能够指导初级、中级技术人员，实施数据库系统的安装、配置、加固与应急处置	4.1.1 培训相关流程和规范 4.1.2 项目指导书的编写方法
	4.2指导	4.2.1 能够针对技术人员，进行风险评估/渗透测试工作的讲解与培训 4.2.2 能够指导初级、中级技术人员，识别检测/评估工作中引入的系统风险，并纠正不当的检测操作	4.2.1 风险评估/渗透测试项目流程与方法 4.2.2 故障分析方法

4 权重表

4.1 理论知识权重表

项目		技能等级		
		初级	中级	高级
		（%）	（%）	（%）
基本要求	职业道德	5	5	5
	基础知识	15	5	3
相关知识	安全事件的监测处置与检测评估	20	50	17
	系统的策略配置与安全加固	50	17	15
	互联网信息安全与网络环境治理	10	15	50
	培训指导	—	4	5
		—	4	5
合计		100	100	100

4.2 技能要求权重表

项目		技能等级		
		初级	中级	高级
		（%）	（%）	（%）
技能要求	安全事件的监测处置与检测评估	30	50	20
	系统的策略配置与安全加固	55	22	15
	互联网信息安全与网络环境治理	15	20	50
	培训指导	—	8	15
合计		100	100	100

附录：

本《标准》修订工作基于以下法律、行政法规及行政规章等，援引如下。

一、法律

《中华人民共和国宪法》第 40 条：中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。

根据《中华人民共和国宪法》第二十五条规定：国家建设网络与信息安全保障体系，提升网络与信息安全保护能力，加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

《中华人民共和国刑法》第 124 条（破坏广播电视设施、公用电信设施罪）：破坏广播电视设施、公用电信设施，危害公共安全的，处三年以上七年以下有期徒刑；造成严重后果的，处七年以上有期徒刑。 过失犯前款罪的，处三年以上七年以下有期徒刑；情节较轻的，处三年以下有期徒刑或者拘役。

《中华人民共和国网络安全法》是为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定的法律。由全国人民代表大会常务委员会于 2016 年 11 月 7 日发布，自 2017 年 6 月 1 日起施行。中华人民共和国主席令（第五十三号）公布。

《中华人民共和国保守国家秘密法》是为了保守国家秘密，维护国家安全和利益，保障改革开放和社会主义建设事业的顺利进行，制定的法律。

《中华人民共和国反恐怖主义法》对电信业务经营者、互联网服务提供者提出了以下要求：

第十八条　电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法进行防范、调查恐怖活动提供技术接口和解密等技术支持和协助。

第十九条　电信业务经营者、互联网服务提供者应当依照法律、行政法规规定，落实网络安全、信息内容监督制度和安全技术防范措施，防止含有恐怖主义、极端主义内容的信息传播；发现含有恐怖主义、极端主义内容的信息的，应当立即停止传输，保存相关记录，删除相关信息，并向公安机关或者有关部门报告。

第二十一条　电信、互联网、金融、住宿、长途客运、机动车租赁等业务经营者、服务提供者，应当对客户身份进行查验。对身份不明或者拒绝身份查验的，不得提供服务。

二、行政条例

《中华人民共和国电信条例》是为了规范电信市场秩序，维护电信用户和电信业务经营者的合法权益，保障电信网络和信息的安全，促进电信业的健康发展，制定的条例。

《国家网络安全事件应急预案》是为了建立健全国家网络安全事件应急工作机制，提高应对网络安全事件能力，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序，制定的条例。

三、行政规章

根据国务院赋予工业和信息化部的相关职能，工业和信息化部在网络与信息安全方面具有组织拟订电信网、互联网及其相关网络与信息安全规划、政策和标准并组织实施；承担电信网、互联网网络与信息安全技术平台的建设和使用管理；承担电信和互联网行业网络安全审查相关工作，组织推动电信网、互联网安全自主可控工作；承担建立电信网、互联网新技术新业务安全评估制度并组织实施；指导督促电信企业和互联网企业落实网络与信息安全管理责任，组织开展网络环境和信息治理，配合处理网上有害信息，配合打击网络犯罪和防范网络失窃密；拟订电信网、互联网网络安全防护政策并组织实施；承担电信网、互联网网络与信息安全监测预警、威胁治理、信息通报和应急管理与处置；承担电信网、互联网网络数据和用户信息安全保护管理工作；承担特殊通信管理，拟订特殊通信、通信管制和网络管制的政策、标准等的职能。

《中华人民共和国行政许可法》和《中华人民共和国行政处罚法》赋予了工业和信息化部及各省通信管理局对电信和互联网行业实施行政许可、行政处罚及信用管理等的行政执法监督权。目前工业和信息化部已颁布的主要相关行政规章有：

《电信服务规范》是为了提高电信服务的质量，维护电信用户的合法权利，保证电信服务和监管工作的系统化和规范化，依据《中华人民共和国电信条例》，制定的规范。

《公用电信网间互联管理规定》是为了维护国家利益和电信用户的合法权益，保护电信业务经营者之间公平、有效竞争，保障公用电信网间及时、合理地互联，根据《中华人民共和国电信条例》，制定的规定。

《电信设备进网管理办法》是为了保证公用电信网的安全畅通，加强电信设备进网管理，维护电信用户和电信业务经营者的合法权益，根据《中华人民共和国电信条例》，制定的办法。

《电信业务经营许可管理办法》是为了加强电信业务经营许可管理，根据《中华人民共和国电信条例》及其他法律、行政法规的规定，制定的办法。

《通信网络安全防护管理办法》是为了加强对通信网络安全的管理，提高通信网络安全防护能力，保障通信网络安全畅通，根据《中华人民共和国电信条例》，制定的办法。通信网络安全防护工作坚持积极防御、综合防范、分级保护的原则。

《电信和互联网用户个人信息保护规定》是为了保护电信和互联网用户的合法权益，维护网络信息安全，根据《全国人民代表大会常务委员会关于加强网络信息保护的决定》、《中华人民共和国电信条例》和《互联网信息服务管理办法》等法律、行政法规，制定的规定。工业和信息化部和各省、自治区、直辖市通信管理局（以下统称电信管理机构）依法对电信和互联网用户个人信息保护工作实施监督管理。

《电信网和互联网管理安全等级保护要求》标准规定了公众电信网和互联网的管理安全登记保护要求。本标准适用于电信网和互联网安全防护体系中的各种网络和系统。

四、其他相关法律、行政法规及行政规章等

《中华人民共和国电子签名法》

《全国人大常委会关于维护互联网安全的决定》

《全国人民代表大会常务委员会关于加强网络信息保护的决定》

《中华人民共和国消费者权益保护法》

《中华人民共和国反不正当竞争法》

《互联网信息服务管理办法》

《国家信息化领导小组关于加强信息安全保障工作的意见》

《计算机信息系统安全保护条例》

《中华人民共和国无线电管理条例》

《商用密码管理条例》

《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》

《信息系统灾难恢复规范》

《电信网间互联争议处理办法》

《通信建设工程质量监督管理规定》

《电信业务经营许可管理办法》

《中华人民共和国无线电频率划分规定》

《电信建设管理办法》

《通信网络安全防护管理办法》

《公共互联网网络安全突发事件应急预案》

《电信和互联网用户个人信息保护规定》

《非经营性互联网信息服务备案管理办法》

《互联网 IP 地址备案管理办法》

《卫星移动通信系统终端地球站管理办法》

《规范互联网信息服务市场秩序若干规定》

《业余无线电台管理办法》

《电话用户真实身份信息登记规定》

《电信网码号资源管理办法》

《电信设备进网管理办法》

《公用电信网间互联管理规定》

《电信服务质量监督管理暂行办法》

《通信短信息服务管理规定》

《互联网电子邮件服务管理办法》

《互联网域名管理办法》

《通信行政处罚程序规定》

《移动互联网应用程序信息服务管理规定》

《网络产品和服务安全审查办法》

《信息安全等级保护 1.0》

《网络安全等级保护制度 2.0》

《电信网和互联网管理安全等级保护要求》

《电信网和互联网管理安全等级保护实施指南》

《GB/T20984》

《电信网和互联网风险评估实施指南》