武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2024年第2期 总第4期

内部资料 电子样本

武汉市网络安全协会简介

INTRODUCTION TO WUHAN CYBER SECURITY ASSOCIATION

武汉市网络安全协会（中文简称：武网安协，英文简称：WHCSA）成立于 2018 年，是在中共武汉市委网络安全和信息化委员会办公室（武汉市互联网信息办公室）主管下，在民政部门依法登记成立的社会团体法人单位，也是唯一代表武汉网络安全产业的专业性组织。

我会是 AAAA 级社会组织；中国网络社会组织联合会、中国网络空间安全协会和中国网络安全产业联盟正式成员单位，全国基础软件安全可信行业产教融合共同体常务副理事长单位，武汉市互联网行业联合会副会长单位；具备全国团体标准信息平台团体标准发布资格；主办有全国首个“移动应用安全公益检测平台”，并与武汉东湖科技保险发展促进中心共建有“东湖网络安全保险服务中心”；配合市人社，市人事考试院针对会员单位组织开展职称评定的申报及审核工作；成立了华中第一个智能汽车网络安全专业委员会、网络安全保险工作委员会和民办高校工作委员会；拥有全市最大最全的网络安全高级专家智库，长期为各级主管部门提供智力支撑。

我会坚持带领成员单位积极主动对接国家互联网应急中心、全国信息安全标准化技术委员会、国家工业信息安全发展研究中心、工信部人才交流中心、工信部第五研究所等国家级平台资源；并与北京、上海、广东、浙江、四川、昆明等兄弟省市网络安全协会广泛开展交流合作；参与了省市网络安全领域各类的课题研究、政策咨询与制定工作；参与并组织历年省市“国家网络安全宣传周”系列宣传活动；主办承办了各类型专业性论坛、赛事、全市攻防演练等大型活动；协助主管部门遴选两年一度的“武汉市网络安全应急技术支撑单位”和每年的网络安全领域“武汉英才”计划培育支持专项等重要工作。

协会的宗旨：遵守宪法、法律、法规和国家政策，践行社会主义核心价值观，遵守社会道德风尚；根据武汉市信息化建设发展的需要，贯彻执行国家的有关法律、法规和政策；以服务社会和服务会员为宗旨，发挥政府管理部门与信息系统用户之间的桥梁和纽带作用；协助管理机关规范和加强系统安全保护工作的管理，协助维护我市网络系统的安全和稳定；推动网络安全技术的发展，促进信息网络用户的法制观念和安全意识的提高，保障我市信息化建设的健康发展。

武汉，是全国首个拥有“国家网络安全人才与创新基地”的超大型国家中心城市，它还拥有着全国前三的高等教育资源、九省通衢的交通区位、上下游完整的产业基础、敢为人先的城市品格等诸多特色优势。《武汉市国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》明确提出，网络安全将成为武汉未来六大新兴产业，得到全市重点发展和布局。

相信未来，在全体武汉网安人的共同努力下，武汉网络安全产业和科技创新必将迎来更加快速、健康、持续的发展，共同为全国网络安全和信息化事业贡献“武汉网络安全”集体力量！

卷首语

“网络安全是事关国家安全和经济社会发展、事关广大人民群众利益的战略问题。”在新技术蓬勃发展、数字经济高速增长及“新质生产力”战略推进的新时期，网络安全风险与挑战日益凸显。“网络”已实质成为人们工作、家庭之外的“第三空间”，但开放共享的网络环境，边界模糊，缺乏有效手段全面排查热点威胁和定位漏洞；组织数据量剧增进一步加大核心数据泄露风险；人工智能带来新的安全漏洞，防止其恶意使用成为新挑战。

新时代网络安全挑战与风险在在汽车行业体现得尤为明显。在“智能化、网联化、共享化、电动化”的引领下，我国新能源汽车高速发展，已经成为当前以及未来汽车发展的主流。智能化网联化的“新汽车”和直连用户的新生态模式，为网络安全注入了新的内容，主要表现在：一、“车 - 路 - 云”协同用车方式，以“车”为核心的网络攻防战随之而来，“车端”成为新的网络安全阵地；二、直连用户模式下企业经营和车端交互留存大量用户信息，相应的个人隐私保护是企业除了核心数据保护、业务连续性保障之外的新的数据安全管理重点；三、中国汽车已大步走向世界，但海外严苛的数据安全和个人信息保护要求是出海企业首先要研究和克服的关键要素之一；四、企业业务“云化”，进一步模糊和无限蔓延信息安全边界，“云计算”加剧了产业链各环节的互粘和依赖，安全威胁和问题越发“一发动全身”。

汽车产业是湖北省、武汉市的支柱产业之一。武汉市网络安全协会智能汽车网络安全专委会成立运行一年多来，在主管部门的精心指导与大力支持下，在各专委会成员单位的协力推动下，已较好起到了武汉市智能网联汽车网络安全领域的协调推进平台作用。新的发展时期，我们将协同各方力量，积极开展广泛的技术交流与“政 - 校 - 企”合作，持续推动智能汽车网络安全领域健康发展，强化网络安全防护体系建设，提升行业整体安全水平，为打造更加安全、可靠的智能汽车生态环境贡献智慧与力量，以实际行动助力武汉智能汽车产业发展阔步前行。

武汉市网络安全协会智能汽车网络安全专业委员会主任、

岚图汽车科技有限公司数字化高级总监：

目 录

CATALOGUE

标准化工作

协会动态

促进和规范数据跨境流动规定

（2024 年 3 月 22 日国家互联网信息办公室令第 16 号）

第一条 为了保障数据安全，保护个人信息权益，促进数据依法有序自由流动，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律法规，对于数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的施行，制定本规定。

第二条 数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

第三条 国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第四条 数据处理者在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第五条 数据处理者向境外提供个人信息，符合下列条件之一的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

（一）为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的；

（二）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

（三）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

（四）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供不满 10 万人个人信息（不含敏感个人信息）的。

前款所称向境外提供的个人信息，不包括重要数据。

第六条 自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单（以下简称负面清单），经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。

自由贸易试验区内数据处理者向境外提供负面清

单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第七条 数据处理者向境外提供数据，符合下列条件之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：

（一）关键信息基础设施运营者向境外提供个人信息或者重要数据；

（二）关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第八条 关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息的，应当依法与境外接收方订立个人信息出境标准合同或者通过个人信息保护认证。

属于本规定第三条、第四条、第五条、第六条规定情形的，从其规定。

第九条 通过数据出境安全评估的结果有效期为 3 年，自评估结果出具之日起计算。有效期届满，需要继续开展数据出境活动且未发生需要重新申报数据出境安全评估情形的，数据处理者可以在有效期届满前 60 个工作日内通过所在地省级网信部门向国家网信部门提出延长评估结果有效期申请。经国家网信部门批准，可以延长评估结果有效期 3 年。

第十条 数据处理者向境外提供个人信息的，应当按照法律、行政法规的规定履行告知、取得个人单独同意、进行个人信息保护影响评估等义务。

第十一条 数据处理者向境外提供数据的，应当遵守法律、法规的规定，履行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生或者可能发生数据安全事件的，应当采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

第十二条 各地网信部门应当加强对数据处理者数据出境活动的指导监督，健全完善数据出境安全评估制度，优化评估流程；强化事前事中事后全链条全领域监管，发现数据出境活动存在较大风险或者发生数据安全事件的，要求数据处理者进行整改，消除隐患；对拒不改正或者造成严重后果的，依法追究法律责任。

第十三条 2022 年 7 月 7 日公布的《数据出境安全评估办法》（国家互联网信息办公室令第 11 号）、2023 年 2 月 22 日公布的《个人信息出境标准合同办法》（国家互联网信息办公室令第 13 号）等相关规定与本规定不一致的，适用本规定。

第十四条 本规定自公布之日起施行。

互联网政务应用安全管理规定

（2024 年 2 月 19 日中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部制定　2024 年 5 月 15 日发布）

第一章　总则

第一条　为保障互联网政务应用安全，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《党委（党组）网络安全工作责任制实施办法》等，制定本规定。

第二条　各级党政机关和事业单位（简称机关事业单位）建设运行互联网政务应用，应当遵守本规定。

本规定所称互联网政务应用，是指机关事业单位在互联网上设立的门户网站，通过互联网提供公共服务的移动应用程序（含小程序）、公众账号等，以及互联网电子邮件系统。

第三条　建设运行互联网政务应用应当依照有关法律、行政法规的规定以及国家标准的强制性要求，落实网络安全与互联网政务应用“同步规划、同步建设、同步使用”原则，采取技术措施和其他必要措施，防范内容篡改、攻击致瘫、数据窃取等风险，保障互联网政务应用安全稳定运行和数据安全。

第二章　开办和建设

第四条　机关事业单位开办网站应当按程序完成开办审核和备案工作。一个党政机关最多开设一个门户网站。中央机构编制管理部门、国务院电信部门、国务院公安部门加强数据共享，优化工作流程，减少填报材料，缩短开办周期。机关事业单位开办网站，应当将运维和安全保障经费纳入预算。

第五条　一个党政机关网站原则上只注册一个中文域名和一个英文域名，域名应当以“.gov.cn”或“. 政务”为后缀。非党政机关网站不得注册使用“.gov.cn”或“. 政务”的域名。事业单位网站的域名应当以“.cn”或“. 公益”为后缀。机关事业单位不得将已注册的网站域名擅自转让给其他单位或个人使用。

第六条　机关事业单位移动应用程序应当在已备案的应用程序分发平台或机关事业单位网站分发。

第七条　机构编制管理部门为机关事业单位制发专属电子证书或纸质证书。机关事业单位通过应用程序分发平台分发移动应用程序，应当向平台运营者提供电子证书或纸质证书用于身份核验；开办微博、公众号、视频号、直播号等公众账号，应当向平台运营者提供电子证书或纸质证书用于身份核验。

第八条　互联网政务应用的名称优先使用实体机构名称、规范简称，使用其他名称的，原则上采取区域名加职责名的命名方式，并在显著位置标明实体机构名称。具体命名规范由中央机构编制管理部门制定。

第九条　中央机构编制管理部门为机关事业单位设置专属网上标识，非机关事业单位不得使用。

机关事业单位网站应当在首页底部中间位置加注网上标识。中央网络安全和信息化委员会办公室会同中央机构编制管理部门协调应用程序分发平台以及公众账号信息服务平台，在移动应用程序下载页面、公众账号显著位置加注网上标识。

第十条 各地区、各部门应当对本地区、本部门党政机关网站建设进行整体规划，推进集约化建设。

县级党政机关各部门以及乡镇党政机关原则上不单独建设网站，可利用上级党政机关网站平台开设网页、栏目、发布信息。

第十一条 互联网政务应用应当支持开放标准，充分考虑对用户端的兼容性，不得要求用户使用特定浏览器、办公软件等用户端软硬件系统访问。

机关事业单位通过互联网提供公共服务，不得绑定单一互联网平台，不得将用户下载安装、注册使用特定互联网平台作为获取服务的前提条件。

第十二条 互联网政务应用因机构调整等原因需变更开办主体的，应当及时变更域名或注册备案信息。不再使用的，应当及时关闭服务，完成数据归档和删除，注销域名和注册备案信息。

第三章 信息安全

第十三条 机关事业单位通过互联网政务应用发布信息，应当健全信息发布审核制度，明确审核程序，指定机构和在编人员负责审核工作，建立审核记录档案，应当确保发布信息内容的权威性、真实性、准确性、及时性和严肃性，严禁发布违法和不良信息。

第十四条 机关事业单位通过互联网政务应用转载信息，应当与政务等履行职能的活动相关，并评估内容的真实性和客观性。转载页面上要准确清晰标注转载来源网站、转载时间、转载链接等，充分考虑图片、内容等知识产权保护问题。

第十五条 机关事业单位发布信息内容需要链接非互联网政务应用的，应当确认链接的资源与政务等履行职能的活动相关，或属于便民服务的范围；应当定期检查链接的有效性和适用性，及时处置异常链接。党政机关门户网站应当采取技术措施，做到在用户点击链接跳转到非党政机关网站时，予以明确提示。

第十六条 机关事业单位应当采取安全保密防控措施，严禁发布国家秘密、工作秘密，防范互联网政务应用数据汇聚、关联引发的泄密风险。应当加强对互联网政务应用存储、处理、传输工作秘密的保密管理。

第四章 网络和数据安全

第十七条 建设互联网政务应用应当落实网络安全等级保护制度和国家密码应用管理要求，按照有关标准规范开展定级备案、等级测评工作，落实安全建设整改加固措施，防范网络和数据安全风险。

中央和国家机关、地市级以上地方党政机关门户网站，以及承载重要业务应用的机关事业单位网站、互联网电子邮件系统等，应当符合网络安全等级保护第三级安全保护要求。

第十八条 机关事业单位应当自行或者委托具有相应资质的第三方网络安全服务机构，对互联网政务应用网络和数据安全每年至少进行一次安全检测评估。互联网政务应用系统升级、新增功能以及引入新技术新应用，应当在上线前进行安全检测评估。

第十九条 互联网政务应用应当设置访问控制策略。对于面向机关事业单位工作人员使用的功能和互联网电子邮箱系统，应当对接入的 IP 地址段或设备实施访问限制，确需境外访问的，按照白名单方式开通特定时段、特定设备或账号的访问权限。

第二十条 机关事业单位应当留存互联网政务应用相关的防火墙、主机等设备的运行日志，以及应用系统的访问日志、数据库的操作日志，留存时间不少于 1 年，并定期对日志进行备份，确保日志的完整性、可用性。

第二十一条 机关事业单位应当按照国家、行业领域有关数据安全和个人信息保护的要求，对互联网政务应用数据进行分类分级管理，对重要数据、个人信息、商业秘密进行重点保护。

第二十二条 机关事业单位通过互联网政务应用收集的个人信息、商业秘密和其他未公开资料，未经信息提供方同意不得向第三方提供或公开，不得用于履行法定职责以外的目的。

第二十三条 为互联网政务应用提供服务的数据中心、云计算服务平台等应当设在境内。

第二十四条 党政机关建设互联网政务应用采购云计算服务，应当选取通过国家云计算服务安全评估的云平台，并加强对所采购云计算服务的使用管理。

第二十五条 机关事业单位委托外包单位开展互联网政务应用开发和运维时，应当以合同等手段明确外包单位网络和数据安全责任，并加强日常监督管理和考核问责；督促外包单位严格按照约定使用、存储、处理数据。未经委托的机关事业单位同意，外包单位不得转包、分包合同任务，不得访问、修改、披露、利用、转让、销毁数据。

机关事业单位应当建立严格的授权访问机制，操作系统、数据库、机房等最高管理员权限必须由本单位在编人员专人负责，不得擅自委托外包单位人员管理使用；应当按照最小必要原则对外包单位人员进行精细化授权，在授权期满后及时收回权限。

第二十六条 机关事业单位应当合理建设或利用社会化专业灾备设施，对互联网政务应用重要数据和信息系统等进行容灾备份。

第二十七条 机关事业单位应当加强互联网政务应用开发安全管理，使用外部代码应当经过安全检测。建立业务连续性计划，防范因供应商服务变更等对升级改造、运维保障等带来的风险。

第二十八条 互联网政务应用使用内容分发网络（CDN）服务的，应当要求服务商将境内用户的域名解析地址指向其境内节点，不得指向境外节点。

第二十九条 互联网政务应用应当使用安全连接方式访问，涉及的电子认证服务应当由依法设立的电子政务电子认证服务机构提供。

第三十条 互联网政务应用应当对注册用户进行真实身份信息认证。国家鼓励互联网政务应用支持用户使用国家网络身份认证公共服务进行真实身份信息注册。

对与人身财产安全、社会公共利益等相关的互联网政务应用和电子邮件系统，应当采取多因素鉴别提高安全性，采取超时退出、限制登录失败次数、账号与终端绑定等技术手段防范账号被盗用风险，鼓励采用电子证书等身份认证措施。

第五章 电子邮件安全

第三十一条 鼓励各地区、各部门通过统一建设、共享使用的模式，建设机关事业单位专用互联网电子邮件系统，作为工作邮箱，为本地区、本行业机关事业单位提供电子邮件服务。党政机关自建的互联网电子邮件系统的域名应当以“.gov.cn”或“.政务”为后缀，事业单位自建的互联网电子邮件系统的域名应当以“.cn”或“.公益”为后缀。机关事业单位工作人员不得使用工作邮箱违规存储、处理、传输、转发国家秘密。

第三十二条 机关事业单位应当建立工作邮箱账号的申请、发放、变更、注销等流程，严格账号审批登记，定期开展账号清理。

第三十三条 机关事业单位互联网电子邮件系统应当关闭邮件自动转发、自动下载附件功能。

第三十四条 机关事业单位互联网电子邮件系统应当具备恶意邮件（含本单位内部发送的邮件）检测拦截功能，对恶意邮箱账号、恶意邮件服务器 IP 以及恶意邮件主题、正文、链接、附件等进行检测和拦截。应当支持钓鱼邮件威胁情报共享，将发现的钓鱼邮件信息报送至主管部门和属地网信部门，按照有关部门下发的钓鱼邮件威胁情报，配置相应防护策略预置拦截钓鱼邮件。

第三十五条 鼓励机关事业单位基于商用密码技术对电子邮件数据的存储进行安全保护。

第六章 监测预警和应急处置

第三十六条 中央网络安全和信息化委员会办公室会同国务院电信主管部门、公安部门和其他有关部门，组织对地市级以上党政机关互联网政务应用开展安全监测。

各地区、各部门应当对本地区、本行业机关事业单位互联网政务应用开展日常监测和安全检查。

机关事业单位应当建立完善互联网政务应用安全监测能力，实时监测互联网政务应用运行状态和网络

安全事件情况。

第三十七条 互联网政务应用发生网络安全事件时，机关事业单位应当按照有关规定向相关部门报告。

第三十八条 中央网络安全和信息化委员会办公室统筹协调重大网络安全事件的应急处置。

互联网政务应用发生或可能发生网络安全事件时，机关事业单位应当立即启动本单位网络安全应急预案，及时处置网络安全事件，消除安全隐患，防止危害扩大。

第三十九条 机构编制管理部门会同网信部门开展针对假冒仿冒互联网政务应用的扫描监测，受理相关投诉举报。网信部门会同电信主管部门，及时对监测发现或网民举报的假冒仿冒互联网政务应用采取停止域名解析、阻断互联网连接和下线处理等措施。公安部门负责打击假冒仿冒互联网政务应用相关违法犯罪活动。

第七章 监督管理

第四十条 中央网络安全和信息化委员会办公室负责统筹协调互联网政务应用安全管理工作。中央机构编制管理部门负责互联网政务应用开办主体身份核验、名称管理和标识管理工作。国务院电信主管部门负责互联网政务应用域名监督管理和互联网信息服务（ICP）备案工作。国务院公安部门负责监督检查指导互联网政务应用网络安全等级保护和相关安全管理工作。

各地区、各部门承担本地区、本行业机关事业单位互联网政务应用安全管理责任，指定一名负责人分管相关工作，加强对互联网政务应用安全工作的组织领导。

第四十一条 对违反或者未能正确履行本规定相关要求的，按照《党委（党组）网络安全工作责任制实施办法》等文件，依规依纪追究当事人和有关领导的责任。

第八章 附则

第四十二条 列入关键信息基础设施的互联网门户网站、移动应用程序、公众账号，以及电子邮件系统的安全管理工作，参照本规定有关内容执行。

第四十三条 本规定由中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部负责解释。

第四十四条 本规定自 2024 年 7 月 1 日起施行。

网络暴力信息治理规定

国家互联网信息办公室
中华人民共和国公安部
中华人民共和国文化和旅游部
国家广播电视总局
令
第 17 号

《网络暴力信息治理规定》已经 2023 年 12 月 25 日国家互联网信息办公室 2023 年第 28 次室务会会议审议通过，并经公安部、文化和旅游部、国家广播电视总局同意，现予公布，自 2024 年 8 月 1 日起施行。

国家互联网信息办公室主任 庄荣文
公安部部长 王小洪
文化和旅游部部长 孙业礼
国家广播电视总局局长 曹淑敏
2024 年 6 月 12 日

网络暴力信息治理规定

第一章 总则

第一条 为了治理网络暴力信息，营造良好网络生态，保障公民合法权益，维护社会公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规，制定本规定。

第二条 中华人民共和国境内的网络暴力信息治理活动，适用本规定。

第三条 网络暴力信息治理坚持源头防范、防控结合、标本兼治、协同共治的原则。

第四条 国家网信部门负责统筹协调全国网络暴力信息治理和相关监督管理工作。国务院公安、文化和旅游、广播电视等有关部门依据各自职责开展网络暴力信息的监督管理工作。

地方网信部门负责统筹协调本行政区域内网络暴力信息治理和相关监督管理工作。地方公安、文化和旅游、广播电视等有关部门依据各自职责开展本行政区域内网络暴力信息的监督管理工作。

第五条 鼓励网络相关行业组织加强行业自律，开展网络暴力信息治理普法宣传，督促指导网络信息服务提供者加强网络暴力信息治理并接受社会监督，为遭受网络暴力信息侵害的用户提供帮扶救助等支持。

第二章 一般规定

第六条 网络信息服务提供者和用户应当坚持社会主义核心价值观，遵守法律法规，尊重社会公德和伦理道德，促进形成积极健康、向上向善的网络文化，

维护良好网络生态。

第七条 网络信息服务提供者应当履行网络信息内容管理主体责任，建立完善网络暴力信息治理机制，健全用户注册、账号管理、个人信息保护、信息发布审核、监测预警、识别处置等制度。

第八条 网络信息服务提供者为用户提供信息发布、即时通讯等服务的，应当依法对用户进行真实身份信息认证。用户不提供真实身份信息的，网络信息服务提供者不得为其提供相关服务。

网络信息服务提供者应当加强用户账号信息管理，为遭受网络暴力信息侵害的相关主体提供账号信息认证协助，防范和制止假冒、仿冒、恶意关联相关主体进行违规注册或者发布信息。

第九条 网络信息服务提供者应当制定和公开管理规则、平台公约，与用户签订服务协议，明确网络暴力信息治理相关权利义务，并依法依约履行治理责任。

第十条 任何组织和个人不得制作、复制、发布、传播涉网络暴力违法信息，应当防范和抵制制作、复制、发布、传播涉网络暴力不良信息。

任何组织和个人不得利用网络暴力事件实施蹭炒热度、推广引流等营销炒作行为，不得通过批量注册或者操纵用户账号等形式组织制作、复制、发布、传播网络暴力信息。

明知他人从事涉网络暴力信息违法犯罪活动的，任何组织和个人不得为其提供数据、技术、流量、资金等支持和协助。

第十一条 网络信息服务提供者应当定期发布网络暴力信息治理公告，并将相关工作情况列入网络信息内容生态治理工作年度报告。

第三章 预防预警

第十二条 网络信息服务提供者应当在国家网信部门和国务院有关部门指导下细化网络暴力信息分类标准规则，建立健全网络暴力信息特征库和典型案例样本库，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络暴力信息的识别监测。

第十三条 网络信息服务提供者应当建立健全网络暴力信息预警模型，综合事件类别、针对主体、参与人数、信息内容、发布频次、环节场景、举报投诉等因素，及时发现预警网络暴力信息风险。

网络信息服务提供者发现存在网络暴力信息风险的，应当及时回应社会关切，引导用户文明互动、理性表达，并对异常账号及时采取真实身份信息动态核验、弹窗提示、违规警示、限制流量等措施；发现相关信息内容浏览、搜索、评论、举报量显著增长等情形的，还应当及时向有关部门报告。

第十四条 网络信息服务提供者应当建立健全用户账号信用管理体系，将涉网络暴力信息违法违规情形记入用户信用记录，依法依约降低账号信用等级或者列入黑名单，并据以限制账号功能或者停止提供相关服务。

第四章 信息和账号处置

第十五条 网络信息服务提供者发现涉网络暴力违法信息的，或者在其服务的醒目位置、易引起用户关注的重点环节发现涉网络暴力不良信息的，应当立即停止传输，采取删除、屏蔽、断开链接等处置措施，保存有关记录，向有关部门报告。发现涉嫌违法犯罪的，应当及时向公安机关报案，并提供相关线索，依法配合开展侦查、调查和处置等工作。

第十六条 互联网新闻信息服务提供者应当坚持正确政治方向、舆论导向、价值取向，加强网络暴力信息治理的公益宣传。

互联网新闻信息服务提供者不得通过夸大事实、过度渲染、片面报道等方式采编发布、转载涉网络暴力新闻信息。对互联网新闻信息提供跟帖评论服务的，应当实行先审后发。

互联网新闻信息服务提供者采编发布、转载涉网络暴力新闻信息不真实或者不公正的，应当立即公开更正，消除影响。

第十七条 网络信息服务提供者应当加强网络视听节目、网络表演等服务内容的管理，发现含有网络

暴力信息的网络视听节目、网络表演等服务的，应当及时删除信息或者停止提供相关服务；应当加强对网络直播、短视频等服务的内容审核，及时阻断含有网络暴力信息的网络直播，处置含有网络暴力信息的短视频。

第十八条 网络信息服务提供者应当加强对跟帖评论信息内容的管理，对以评论、回复、留言、弹幕、点赞等方式制作、复制、发布、传播网络暴力信息的，应当及时采取删除、屏蔽、关闭评论、停止提供相关服务等处置措施。

第十九条 网络信息服务提供者应当加强对网络论坛社区和网络群组的管理，禁止用户在版块、词条、超话、群组等环节制作、复制、发布、传播网络暴力信息，禁止以匿名投稿、隔空喊话等方式创建含有网络暴力信息的论坛社区和群组账号。

网络论坛社区、网络群组的建立者和管理者应当履行管理责任，发现用户制作、复制、发布、传播网络暴力信息的，应当依法依约采取限制发言、移出群组等管理措施。

第二十条 公众账号生产运营者应当建立健全发布推广、互动评论等全过程信息内容安全审核机制，发现账号跟帖评论等环节存在网络暴力信息的，应当及时采取举报、处置等措施。

第二十一条 对违反本规定第十条的用户，网络信息服务提供者应当依法依约采取警示、删除信息、限制账号功能、关闭账号等处置措施，并保存相关记录；对组织、煽动、多次发布网络暴力信息的，网络信息服务提供者还应当依法依约采取列入黑名单、禁止重新注册等处置措施。

对借网络暴力事件实施营销炒作等行为的，除前款规定外，还应当依法依约采取清理订阅关注账号、暂停营利权限等处置措施。

第二十二条 对组织、煽动制作、复制、发布、传播网络暴力信息的网络信息内容多渠道分发服务机构，网络信息服务提供者应当依法依约对该机构及其管理的账号采取警示、暂停营利权限、限制提供服务、入驻清退等处置措施。

第五章 保护机制

第二十三条 网络信息服务提供者应当建立健全网络暴力信息防护功能，提供便利用户设置屏蔽陌生用户或者特定用户、本人发布信息可见范围、禁止转载或者评论本人发布信息等网络暴力信息防护选项。

网络信息服务提供者应当完善私信规则，提供便利用户设置仅接收好友私信或者拒绝接收所有私信等网络暴力信息防护选项，鼓励提供智能屏蔽私信或者自定义私信屏蔽词等功能。

第二十四条 网络信息服务提供者发现用户面临网络暴力信息风险的，应当及时通过显著方式提示用户，告知用户可以采取的防护措施。

网络信息服务提供者发现网络暴力信息风险涉及以下情形的，还应当为用户提供网络暴力信息防护指导和保护救助服务，协助启动防护措施，并向网信、公安等有关部门报告：

（一）网络暴力信息侵害未成年人、老年人、残疾人等用户合法权益的；

（二）网络暴力信息侵犯用户个人隐私的；

（三）若不及时采取措施，可能造成用户人身、财产损害等严重后果的其他情形。

第二十五条 网络信息服务提供者发现、处置网络暴力信息的，应当及时保存信息内容、浏览评论转发数量等数据。网络信息服务提供者应当向用户提供网络暴力信息快捷取证等功能，依法依约为用户维权提供便利。

公安、网信等有关部门依法调取证据的，网络信息服务提供者应当及时提供必要的技术支持和协助。

第二十六条 网络信息服务提供者应当自觉接受社会监督，优化投诉、举报程序，在服务显著位置设置专门的网络暴力信息快捷投诉、举报入口，公布处理流程，及时受理、处理公众投诉、举报并反馈处理结果。

网络信息服务提供者应当结合投诉、举报内容以及相关证明材料及时研判。对属于网络暴力信息的投诉、

举报，应当依法处理并反馈结果；对因证明材料不充分难以准确判断的，应当及时告知用户补充证明材料；对不属于网络暴力信息的投诉、举报，应当按照其他类型投诉、举报的受理要求予以处理并反馈结果。

第二十七条 网络信息服务提供者应当优先处理涉未成年人网络暴力信息的投诉、举报。发现涉及侵害未成年人用户合法权益的网络暴力信息风险的，应当按照法律法规和本规定要求及时采取措施，提供相应保护救助服务，并向有关部门报告。

网络信息服务提供者应当设置便利未成年人及其监护人行使通知删除网络暴力信息权利的功能、渠道，接到相关通知后，应当及时采取删除、屏蔽、断开链接等必要的措施，防止信息扩散。

第六章 监督管理和法律责任

第二十八条 网信部门会同公安、文化和旅游、广播电视等有关部门依法对网络信息服务提供者的网络暴力信息治理情况进行监督检查。

网络信息服务提供者对网信部门和有关部门依法实施的监督检查应当予以配合。

第二十九条 网信部门会同公安、文化和旅游、广播电视等有关部门建立健全信息共享、会商通报、取证调证、案件督办等工作机制，协同治理网络暴力信息。

公安机关对于网信、文化和旅游、广播电视等部门移送的涉网络暴力信息违法犯罪线索，应当及时进行审查，并对符合立案条件的及时立案侦查、调查。

第三十条 违反本规定的，依照《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国治安管理处罚法》、《互联网信息服务管理办法》等法律、行政法规的规定予以处罚。

法律、行政法规没有规定的，由网信、公安、文化和旅游、广播电视等有关部门依据职责给予警告、通报批评，责令限期改正，可以并处一万元以上十万元以下罚款；涉及危害公民生命健康安全且有严重后果的，并处十万元以上二十万元以下罚款。

对组织、煽动制作、复制、发布、传播网络暴力信息或者利用网络暴力事件实施恶意营销炒作等行为的组织和个人，应当依法从重处罚。

第三十一条 违反本规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附则

第三十二条 本规定所称网络暴力信息，是指通过网络以文本、图像、音频、视频等形式对个人集中发布的，含有侮辱谩骂、造谣诽谤、煽动仇恨、威逼胁迫、侵犯隐私，以及影响身心健康的指责嘲讽、贬低歧视等内容的违法和不良信息。

第三十三条 依法通过网络检举、揭发他人违法犯罪，或者依法实施舆论监督的，不适用本规定。

第三十四条 本规定自 2024 年 8 月 1 日起施行。

网络数据安全管理条例

中华人民共和国国务院令第 790 号

《网络数据安全管理条例》已经 2024 年 8 月 30 日国务院第 40 次常务会议通过，现予公布，自 2025 年 1 月 1 日起施行。

总理 李强

2024 年 9 月 24 日

网络数据安全管理条例

第一章　总则

第一条　为了规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条　在中华人民共和国境内开展网络数据处理活动及其安全监督管理，适用本条例。

在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，符合《中华人民共和国个人信息保护法》第三条第二款规定情形的，也适用本条例。

在中华人民共和国境外开展网络数据处理活动，损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的，依法追究法律责任。

第三条　网络数据安全管理工作坚持中国共产党的领导，贯彻总体国家安全观，统筹促进网络数据开发利用与保障网络数据安全。

第四条　国家鼓励网络数据在各行业、各领域的创新应用，加强网络数据安全防护能力建设，支持网络数据相关技术、产品、服务创新，开展网络数据安全宣传教育和人才培养，促进网络数据开发利用和产业发展。

第五条　国家根据网络数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，对网络数据实行分类分级保护。

第六条　国家积极参与网络数据安全相关国际规则和标准的制定，促进国际交流与合作。

第七条　国家支持相关行业组织按照章程，制定网络数据安全行为规范，加强行业自律，指导会员加强网络数据安全保护，提高网络数据安全保护水平，促进行业健康发展。

第二章　一般规定

第八条　任何个人、组织不得利用网络数据从事非法活动，不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

任何个人、组织不得提供专门用于从事前款非法活动的程序、工具；明知他人从事前款非法活动的，不得为其提供互联网接入、服务器托管、网络存储、通讯传输等技术支持，或者提供广告推广、支付结算等帮助。

第九条　网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求，在网络安全等级保护的基础上，加强网络数据安全防护，建立健全网络数据安全管理制度，采取加密、备份、访问控制、安全认证等技术措施和其他必要措施，保护网络数据免遭篡改、破坏、泄露或者非法获取、非法利用，处置网络数据安全事件，防范针对和利用网络数据实施的违法犯罪活动，并对所处理网络数据的安全承担主体责任。

第十条　网络数据处理者提供的网络产品、服务应当符合相关国家标准的强制性要求；发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告；涉及危害国家安全、公共利益的，网络数据处理者还应当在 24 小时内向有关主管部门报告。

第十一条　网络数据处理者应当建立健全网络数据安全事件应急预案，发生网络数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

网络数据安全事件对个人、组织合法权益造成危害的，网络数据处理者应当及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知利害关系人；法律、行政法规规定可以不通知的，从其规定。网络数据处理者在处置网络数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

第十二条　网络数据处理者向其他网络数据处理者提供、委托处理个人信息和重要数据的，应当通过合同等与网络数据接收方约定处理目的、方式、范围以及安全保护义务等，并对网络数据接收方履行义务的情况进行监督。向其他网络数据处理者提供、委托处理个人信息和重要数据的处理情况记录，应当至少保存 3 年。

网络数据接收方应当履行网络数据安全保护义务，并按照约定的目的、方式、范围等处理个人信息和重要数据。

两个以上的网络数据处理者共同决定个人信息和重要数据的处理目的和处理方式的，应当约定各自的权利和义务。

第十三条　网络数据处理者开展网络数据处理活动，影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查。

第十四条　网络数据处理者因合并、分立、解散、破产等原因需要转移网络数据的，网络数据接收方应当继续履行网络数据安全保护义务。

第十五条　国家机关委托他人建设、运行、维护电子政务系统，存储、加工政务数据，应当按照国家有关规定经过严格的批准程序，明确受托方的网络数据处理权限、保护责任等，监督受托方履行网络数据安全保护义务。

第十六条　网络数据处理者为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，应当依照法律、法规的规定和合同约定履行网络数据安全保护义务，提供安全、稳定、持续的服务。

前款规定的网络数据处理者未经委托方同意，不得访问、获取、留存、使用、泄露或者向他人提供网络数据，不得对网络数据进行关联分析。

第十七条　为国家机关提供服务的信息系统应当参照电子政务系统的管理要求加强网络数据安全管理，保障网络数据安全。

第十八条　网络数据处理者使用自动化工具访问、

收集网络数据，应当评估对网络服务带来的影响，不得非法侵入他人网络，不得干扰网络服务正常运行。

第十九条 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理，采取有效措施防范和处置网络数据安全风险。

第二十条 面向社会提供产品、服务的网络数据处理者应当接受社会监督，建立便捷的网络数据安全投诉、举报渠道，公布投诉、举报方式等信息，及时受理并处理网络数据安全投诉、举报。

第三章 个人信息保护

第二十一条 网络数据处理者在处理个人信息前，通过制定个人信息处理规则的方式依法向个人告知的，个人信息处理规则应当集中公开展示、易于访问并置于醒目位置，内容明确具体、清晰易懂，包括但不限于下列内容：

（一）网络数据处理者的名称或者姓名和联系方式；

（二）处理个人信息的目的、方式、种类，处理敏感个人信息的必要性以及对个人权益的影响；

（三）个人信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法；

（四）个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。

网络数据处理者按照前款规定向个人告知收集和向其他网络数据处理者提供个人信息的目的、方式、种类以及网络数据接收方信息的，应当以清单等形式予以列明。网络数据处理者处理不满十四周岁未成年人个人信息的，还应当制定专门的个人信息处理规则。

第二十二条 网络数据处理者基于个人同意处理个人信息的，应当遵守下列规定：

（一）收集个人信息为提供产品或者服务所必需，不得超范围收集个人信息，不得通过误导、欺诈、胁迫等方式取得个人同意；

（二）处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息的，应当取得个人的单独同意；

（三）处理不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的同意；

（四）不得超出个人同意的个人信息处理目的、方式、种类、保存期限处理个人信息；

（五）不得在个人明确表示不同意处理其个人信息后，频繁征求同意；

（六）个人信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。

法律、行政法规规定处理敏感个人信息应当取得书面同意的，从其规定。

第二十三条 个人请求查阅、复制、更正、补充、删除、限制处理其个人信息，或者个人注销账号、撤回同意的，网络数据处理者应当及时受理，并提供便捷的支持个人行使权利的方法和途径，不得设置不合理条件限制个人的合理请求。

第二十四条 因使用自动化采集技术等无法避免采集到非必要个人信息或者未依法取得个人同意的个人信息，以及个人注销账号的，网络数据处理者应当删除个人信息或者进行匿名化处理。法律、行政法规规定的保存期限未届满，或者删除、匿名化处理个人信息从技术上难以实现的，网络数据处理者应当停止除存储和采取必要的安全保护措施之外的处理。

第二十五条 对符合下列条件的个人信息转移请求，网络数据处理者应当为个人指定的其他网络数据处理者访问、获取有关个人信息提供途径：

（一）能够验证请求人的真实身份；

（二）请求转移的是本人同意提供的或者基于合同收集的个人信息；

（三）转移个人信息具备技术可行性；

（四）转移个人信息不损害他人合法权益。

请求转移个人信息次数等明显超出合理范围的，网络数据处理者可以根据转移个人信息的成本收取必要费用。

第二十六条 中华人民共和国境外网络数据处理者处理境内自然人个人信息，依照《中华人民共和国

个人信息保护法》第五十三条规定在境内设立专门机构或者指定代表的，应当将有关机构的名称或者代表的姓名、联系方式等报送所在地设区的市级网信部门；网信部门应当及时通报同级有关主管部门。

第二十七条 网络数据处理者应当定期自行或者委托专业机构对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第二十八条 网络数据处理者处理 1000 万人以上个人信息的，还应当遵守本条例第三十条、第三十二条对处理重要数据的网络数据处理者（以下简称重要数据的处理者）作出的规定。

第四章 重要数据安全

第二十九条 国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的网络数据进行重点保护。

网络数据处理者应当按照国家有关规定识别、申报重要数据。对确认为重要数据的，相关地区、部门应当及时向网络数据处理者告知或者公开发布。网络数据处理者应当履行网络数据安全保护责任。

国家鼓励网络数据处理者使用数据标签标识等技术和产品，提高重要数据安全管理水平。

第三十条 重要数据的处理者应当明确网络数据安全负责人和网络数据安全管理机构。网络数据安全管理机构应当履行下列网络数据安全保护责任：

（一）制定实施网络数据安全管理制度、操作规程和网络数据安全事件应急预案；

（二）定期组织开展网络数据安全风险监测、风险评估、应急演练、宣传教育培训等活动，及时处置网络数据安全风险和事件；

（三）受理并处理网络数据安全投诉、举报。

网络数据安全负责人应当具备网络数据安全专业知识和相关管理工作经历，由网络数据处理者管理层成员担任，有权直接向有关主管部门报告网络数据安全情况。

掌握有关主管部门规定的特定种类、规模的重要数据的网络数据处理者，应当对网络数据安全负责人和关键岗位的人员进行安全背景审查，加强相关人员培训。审查时，可以申请公安机关、国家安全机关协助。

第三十一条 重要数据的处理者提供、委托处理、共同处理重要数据前，应当进行风险评估，但是属于履行法定职责或者法定义务的除外。

风险评估应当重点评估下列内容：

（一）提供、委托处理、共同处理网络数据，以及网络数据接收方处理网络数据的目的、方式、范围等是否合法、正当、必要；

（二）提供、委托处理、共同处理的网络数据遭到篡改、破坏、泄露或者非法获取、非法利用的风险，以及对国家安全、公共利益或者个人、组织合法权益带来的风险；

（三）网络数据接收方的诚信、守法等情况；

（四）与网络数据接收方订立或者拟订立的相关合同中关于网络数据安全的要求能否有效约束网络数据接收方履行网络数据安全保护义务；

（五）采取或者拟采取的技术和管理措施等能否有效防范网络数据遭到篡改、破坏、泄露或者非法获取、非法利用等风险；

（六）有关主管部门规定的其他评估内容。

第三十二条 重要数据的处理者因合并、分立、解散、破产等可能影响重要数据安全的，应当采取措施保障网络数据安全，并向省级以上有关主管部门报告重要数据处置方案、接收方的名称或者姓名和联系方式等；主管部门不明确的，应当向省级以上数据安全工作协调机制报告。

第三十三条 重要数据的处理者应当每年度对其网络数据处理活动开展风险评估，并向省级以上有关主管部门报送风险评估报告，有关主管部门应当及时通报同级网信部门、公安机关。

风险评估报告应当包括下列内容：

（一）网络数据处理者基本信息、网络数据安全管

理机构信息、网络数据安全负责人姓名和联系方式等；

（二）处理重要数据的目的、种类、数量、方式、范围、存储期限、存储地点等，开展网络数据处理活动的情况，不包括网络数据内容本身；

（三）网络数据安全管理制度及实施情况，加密、备份、标签标识、访问控制、安全认证等技术措施和其他必要措施及其有效性；

（四）发现的网络数据安全风险，发生的网络数据安全事件及处置情况；

（五）提供、委托处理、共同处理重要数据的风险评估情况；

（六）网络数据出境情况；

（七）有关主管部门规定的其他报告内容。

处理重要数据的大型网络平台服务提供者报送的风险评估报告，除包括前款规定的内容外，还应当充分说明关键业务和供应链网络数据安全等情况。

重要数据的处理者存在可能危害国家安全的重要数据处理活动的，省级以上有关主管部门应当责令其采取整改或者停止处理重要数据等措施。重要数据的处理者应当按照有关要求立即采取措施。

第五章　网络数据跨境安全管理

第三十四条　国家网信部门统筹协调有关部门建立国家数据出境安全管理专项工作机制，研究制定国家网络数据出境安全管理相关政策，协调处理网络数据出境安全重大事项。

第三十五条　符合下列条件之一的，网络数据处理者可以向境外提供个人信息：

（一）通过国家网信部门组织的数据出境安全评估；

（二）按照国家网信部门的规定经专业机构进行个人信息保护认证；

（三）符合国家网信部门制定的关于个人信息出境标准合同的规定；

（四）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；

（五）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息；

（六）为履行法定职责或者法定义务，确需向境外提供个人信息；

（七）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息

（八）法律、行政法规或者国家网信部门规定的其他条件。

第三十六条　中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

第三十七条　网络数据处理者在中华人民共和国境内运营中收集和产生的重要数据确需向境外提供的，应当通过国家网信部门组织的数据出境安全评估。网络数据处理者按照国家有关规定识别、申报重要数据，但未被相关地区、部门告知或者公开发布为重要数据的，不需要将其作为重要数据申报数据出境安全评估。

第三十八条　通过数据出境安全评估后，网络数据处理者向境外提供个人信息和重要数据的，不得超出评估时明确的数据出境目的、方式、范围和种类、规模等。

第三十九条　国家采取措施，防范、处置网络数据跨境安全风险和威胁。任何个人、组织不得提供专门用于破坏、避开技术措施的程序、工具等；明知他人从事破坏、避开技术措施等活动的，不得为其提供技术支持或者帮助。

第六章　网络平台服务提供者义务

第四十条　网络平台服务提供者应当通过平台规则或者合同等明确接入其平台的第三方产品和服务提供者的网络数据安全保护义务，督促第三方产品和服务提供者加强网络数据安全管理。

预装应用程序的智能终端等设备生产者，适用前款规定。

第三方产品和服务提供者违反法律、行政法规的规定或者平台规则、合同约定开展网络数据处理活动，对用户造成损害的，网络平台服务提供者、第三方产

品和服务提供者、预装应用程序的智能终端等设备生产者应当依法承担相应责任。

国家鼓励保险公司开发网络数据损害赔偿责任险种，鼓励网络平台服务提供者、预装应用程序的智能终端等设备生产者投保。

第四十一条 提供应用程序分发服务的网络平台服务提供者，应当建立应用程序核验规则并开展网络数据安全相关核验。发现待分发或者已分发的应用程序不符合法律、行政法规的规定或者国家标准的强制性要求的，应当采取警示、不予分发、暂停分发或者终止分发等措施。

第四十二条 网络平台服务提供者通过自动化决策方式向个人进行信息推送的，应当设置易于理解、便于访问和操作的个性化推荐关闭选项，为用户提供拒绝接收推送信息、删除针对其个人特征的用户标签等功能。

第四十三条 国家推进网络身份认证公共服务建设，按照政府引导、用户自愿原则进行推广应用。

鼓励网络平台服务提供者支持用户使用国家网络身份认证公共服务登记、核验真实身份信息。

第四十四条 大型网络平台服务提供者应当每年度发布个人信息保护社会责任报告，报告内容包括但不限于个人信息保护措施和成效、个人行使权利的申请受理情况、主要由外部成员组成的个人信息保护监督机构履行职责情况等。

第四十五条 大型网络平台服务提供者跨境提供网络数据，应当遵守国家数据跨境安全管理要求，健全相关技术和管理措施，防范网络数据跨境安全风险。

第四十六条 大型网络平台服务提供者不得利用网络数据、算法以及平台规则等从事下列活动：

（一）通过误导、欺诈、胁迫等方式处理用户在平台上产生的网络数据；

（二）无正当理由限制用户访问、使用其在平台上产生的网络数据；

（三）对用户实施不合理的差别待遇，损害用户合法权益；

（四）法律、行政法规禁止的其他活动。

第七章 监督管理

第四十七条 国家网信部门负责统筹协调网络数据安全和相关监督管理工作。

公安机关、国家安全机关依照有关法律、行政法规和本条例的规定，在各自职责范围内承担网络数据安全监督管理职责，依法防范和打击危害网络数据安全的违法犯罪活动。

国家数据管理部门在具体承担数据管理工作中履行相应的网络数据安全职责。

各地区、各部门对本地区、本部门工作中收集和产生的网络数据及网络数据安全负责。

第四十八条 各有关主管部门承担本行业、本领域网络数据安全监督管理职责，应当明确本行业、本领域网络数据安全保护工作机构，统筹制定并组织实施本行业、本领域网络数据安全事件应急预案，定期组织开展本行业、本领域网络数据安全风险评估，对网络数据处理者履行网络数据安全保护义务情况进行监督检查，指导督促网络数据处理者及时对存在的风险隐患进行整改。

第四十九条 国家网信部门统筹协调有关主管部门及时汇总、研判、共享、发布网络数据安全风险相关信息，加强网络数据安全信息共享、网络数据安全风险和威胁监测预警以及网络数据安全事件应急处置工作。

第五十条 有关主管部门可以采取下列措施对网络数据安全进行监督检查：

（一）要求网络数据处理者及其相关人员就监督检查事项作出说明；

（二）查阅、复制与网络数据安全有关的文件、记录；

（三）检查网络数据安全措施运行情况；

（四）检查与网络数据处理活动有关的设备、物品；

（五）法律、行政法规规定的其他必要措施。

网络数据处理者应当对有关主管部门依法开展的网络数据安全监督检查予以配合。

第五十一条 有关主管部门开展网络数据安全监督检查，应当客观公正，不得向被检查单位收取费用。

有关主管部门在网络数据安全监督检查中不得访问、收集与网络数据安全无关的业务信息，获取的信息只能用于维护网络数据安全的需要，不得用于其他用途。

有关主管部门发现网络数据处理者的网络数据处理活动存在较大安全风险的，可以按照规定的权限和程序要求网络数据处理者暂停相关服务、修改平台规则、完善技术措施等，消除网络数据安全隐患。

第五十二条 有关主管部门在开展网络数据安全监督检查时，应当加强协同配合、信息沟通，合理确定检查频次和检查方式，避免不必要的检查和交叉重复检查。

个人信息保护合规审计、重要数据风险评估、重要数据出境安全评估等应当加强衔接，避免重复评估、审计。重要数据风险评估和网络安全等级测评的内容重合的，相关结果可以互相采信。

第五十三条 有关主管部门及其工作人员对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等网络数据应当依法予以保密，不得泄露或者非法向他人提供。

第五十四条 境外的组织、个人从事危害中华人民共和国国家安全、公共利益，或者侵害中华人民共和国公民的个人信息权益的网络数据处理活动的，国家网信部门会同有关主管部门可以依法采取相应的必要措施。

第八章 法律责任

第五十五条 违反本条例第十二条、第十六条至第二十条、第二十二条、第四十条第一款和第二款、第四十一条、第四十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处 100 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主

管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款。

第五十六条 违反本条例第十三条规定的，由网信、电信、公安、国家安全等主管部门依据各自职责责令改正，给予警告，可以并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；拒不改正或者情节严重的，处 100 万元以上 1000 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款。

第五十七条 违反本条例第二十九条第二款、第三十条第二款和第三款、第三十一条、第三十二条规定的，由网信、电信、公安等主管部门依据各自职责责令改正，给予警告，可以并处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员可以处 1 万元以上 10 万元以下罚款；拒不改正或者造成大量数据泄露等严重后果的，处 50 万元以上 200 万元以下罚款，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处 5 万元以上 20 万元以下罚款。

第五十八条 违反本条例其他有关规定的，由有关主管部门依照《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信

息保护法》等法律的有关规定追究法律责任。

第五十九条 网络数据处理者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。

第六十条 国家机关不履行本条例规定的网络数据安全保护义务的，由其上级机关或者有关主管部门责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第六十一条 违反本条例规定，给他人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第九章 附则

第六十二条 本条例下列用语的含义：

（一）网络数据，是指通过网络处理和产生的各种电子数据。

（二）网络数据处理活动，是指网络数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

（三）网络数据处理者，是指在网络数据处理活动中自主决定处理目的和处理方式的个人、组织。

（四）重要数据，是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

（五）委托处理，是指网络数据处理者委托个人、组织按照约定的目的和方式开展的网络数据处理活动。

（六）共同处理，是指两个以上的网络数据处理者共同决定网络数据的处理目的和处理方式的网络数据处理活动。

（七）单独同意，是指个人针对其个人信息进行特定处理而专门作出具体、明确的同意。

（八）大型网络平台，是指注册用户 5000 万以上或者月活跃用户 1000 万以上，业务类型复杂，网络数据处理活动对国家安全、经济运行、国计民生等具有重要影响的网络平台。

第六十三条 开展核心数据的网络数据处理活动，按照国家有关规定执行。

自然人因个人或者家庭事务处理个人信息的，不适用本条例。

开展涉及国家秘密、工作秘密的网络数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

第六十四条 本条例自 2025 年 1 月 1 日起施行。

庆七一学党章强信念 铸网盾践初心谱新篇

——武汉市网络安全协会党支部与湖北东方网盾信息安全技术有限公司党支部举办七一联合党日活动成功举办

提要：武汉市网络安全协会党支部与湖北东方网盾信息安全技术有限公司党支部联合举办七一主题党日活动，共同探讨和推进党建工作，加强社会组织及非公经济党组织的建设，推动协会与企业党建工作健康发展。党员们结合工作实际和自身经历，积极发言，分享对党建工作的理解和感悟。活动旨在加强党性修养，进一步推动社会组织和企业党建工作，为实现中华民族伟大复兴的中国梦贡献力量。

7 月 1 日，为庆祝中国共产党成立 103 周年，武汉市网络安全协会党支部与协会理事单位湖北东方网盾信息安全技术有限公司党支部携手举办了一场主题为“庆七一学党章强信念 铸网盾践初心谱新篇”的主题党日活动。在此次的活动中，党员们共同探讨和推进党建工作，并以此为指导，全面加强了社会组织及非公经济党组织的建设，进一步推动了协会与企业党建工作的健康发展。

活动在武汉市网络安全协会会议室举行。活动伊始，在协会支部书记的带领下，全体党员共同重温入党誓词，表达对党的忠诚和对共产主义事业的坚定信念。

全体党员举起右拳，重温入党誓词

随后，党员们集中探讨了社会组织与非公经济党建工作的新思路和新方法，集体学习了《党章》，观看了人民网制作系列党校公开课视频和相关指导资料。通过学习，各党员深刻意识到加强社会组织党建工作，对于引领社会组织正确发展方向，激发社会组织活力，促进社会组织在国家治理体系和治理能力现代化进程中更好发挥作用，对于把社会组织及其从业人员紧密团结在党的周围，不断扩大党在社会组织的影响力，增强党的阶级基础、扩大党的群众基础、夯实党的执政基础，都具有重要意义。

在交流环节，党员们结合工作实际和自身经历，积极发言，分享了对党建工作的理解和感悟。

武汉市网络安全协会党支部委员雷侃表示："党建工作需要我们不断创新和完善，以适应新时代的发展要求。作为行业内的一名党员，在日常工作过程中，应该利用自己专业特长，积极参与党建工作，为党的事业贡献自己的力量。"

湖北东方网盾信息安全技术有限公司党支部党员扈莎莎表示："党建工作的关键在于提高我们的政治觉悟和组织纪律性。我们要做到有所敬畏，严守政治纪律和政治规矩，从细节做起，从小事做起，提高自身素质，做一名优秀合格的共产党员。"

湖北东方网盾信息安全技术有限公司党支部党员万威结合公司实际情况谈道："在公司业务中，我们也要将党建精神融入其中，始终追求公正客观专业，真实准确测评系统安全情况，我们党员更要实事求是，不忘初心，砥砺前行。"

大家纷纷表示，要加强党性修养，积极推动社会组织和企业党建工作，为实现中华民族伟大复兴的中国梦贡献力量。

武汉市网络安全协会党支部书记、秘书长刘悦恒总结道："通过本次学习，我们都深刻认识到党建工作对于推进全面从严治党和加强党的建设具有重要意义。我们将积极组织支部党员开展党章学习和党建工作，加强党性教育，引导协会及所有会员单位的党员干部积极参与党建工作，确保全体党员在思想上、行动上始终与党中央保持高度一致。"

武汉市互联网行业党委党建指导员何溪山代表上级党组织表示："通过此次联合党日活动，不仅增强了党员们的党性修养，也深化了党组织间的交流合作。希

望两个党支部能继续保持这种热情与活力，持续加强党员的教育和培训，深刻领悟‘两个确立’、坚决做到‘两个维护’的重要意义。希望未来的党建工作中，更加注重理论与实践相结合，将党的理论与网络安全行业的实际工作紧密联系起来，同时，也要积极探索新的党建模式和方法，提高党建工作的针对性和实效性。”

活动的最后，全体党员集体参观了八七会议会址。在这处见证了中国共产党历史上重要转折点的革命遗址，党员们深刻感受到历史的厚重和身负的时代责任。

八七会议是中国共产党历史上一次重要会议，它在中国革命遭受严重挫折后，总结了失败的经验教训，结束了陈独秀的右倾机会主义在党中央的统治，确定了党领导武装暴动、开展土地革命的斗争方针。这次会议对于挽救大革命失败所造成的危局，实现党的战略转变起了重要作用。

武汉市网络安全协会党支部党员张玉萍参观后表示：“站在八七会议会址，我仿佛能听到历史的回声，感受到革命先烈的英勇和牺牲。这更加坚定了我要为网信事业贡献力量的决心。”

湖北东方网盾信息安全技术有限公司支部党员孙菊蓉感叹：“我们可以感受到那段激情燃烧的岁月，体味到革命先辈们为了国家和人民的福祉所付出的巨大牺牲。在这里，我们可以缅怀革命先辈们的丰功伟绩，也应该汲取他们的精神力量，为实现中华民族伟大复兴的中国梦而努力奋斗。”

此次联合党日活动不仅增强了党员的党性修养和凝聚力，也促进了两个党支部之间的交流合作。通过深入探讨党建工作，党员们对党的历史、党的建设以及非公经济党的建设工作有了更加深刻的认识和理解。未来，武汉市网络安全协会党支部与湖北东方网盾信息安全技术有限公司党支部将继续深化交流合作，共同推动网络安全事业和社会组织党建工作的发展，为奋力推进中国式现代化武汉实践提供有力服务、支撑和保障。

武汉市网络安全协会党支部慰问硚口区荣华街道防汛抗旱分指挥部

近日，武汉市网络安全协会党支部全体党员及秘书处工作人员赴硚口区荣华街道防汛抗旱分指挥部开展慰问活动，为防汛工作人员们送去深切问候与物资援助。

入夏以来，长江沿岸的防汛形势严峻，在国家省市防汛部门的统一指挥下，一线防汛人员们始终坚守岗位，夜以继日地奋战在长江与汉江堤防上，筑起了一道坚不可摧的安全防线。武汉市网络安全协会代表全市网络安全产业赴硚口区荣华街道开展慰问，向防汛人员们表达深深的敬意与关怀。

协会党支部书记、秘书长刘悦恒带队，与协会多位负责人一同前往防汛现场，不仅送去了饮品、饮料、方便面等生活必需品，还与现场指挥部工作人员进行了深入的交流，详细询问了当前汉江水位状况、人员轮班安排及后勤保障情况，充分展现了网络安全产业对防汛工作的关注与支持。

战胜汛情，全民一心。硚口区荣华街道荣华社区党委书记张望对网安协会一直以来的工作支持表达了衷心的感谢，并表示会全力以赴做好防汛工作，确保汉江流域安全度汛。

此次慰问活动不仅加深了网络安全产业与防汛工作之间的联系，也激发了社会各界共同参与防汛、共筑安全防线的热情。武汉市网络安全协会表示，未来将继续履行社会责任，积极参与各类公益活动，为保障民生安全、促进社会发展贡献更多力量。

“党建引领 融合赋能”市委网信办举行 2024 年集聚区专项服务第七场活动

9 月 10 日，武汉市委网信办 2024 年“党建引领、融合赋能”集聚区专项服务第七场活动在临空港中国网谷产业集聚区举行，活动以网络安全宣讲为主题，30 多名集聚区企业代表参加了本次活动。

活动现场，工作人员向临空港中国网谷产业集聚区企业代表发放了网络安全宣传手册，并以趣味答题的方式宣讲数据安全、关键网络设施安全等相关知识。大家表示，此次活动的开展，提升了自身网络安全防范意识，希望今后多开展类似的活动。

本场活动由武汉市网络安全协会、临空港中国网谷产业集聚区综合党委具体承办，武汉安域信息安全技术有限公司支持。本次活动举办地所在的临空港中国网谷产业集聚区位列全市首批 30 个重点集聚区名录。

武汉地铁桥隧公司党支部与武汉市网络安全协会党支部联合开展主题党日活动

9 月 13 日，武汉地铁桥隧管理有限公司一党支部与武汉市网络安全协会党支部，联合开展 2024 年国家网络安全宣传周主题党日活动。本次活动旨在宣传贯彻总体国家安全观和网络强国战略，深化网络安全意识，强化网络安全责任，构建更加坚固的网络安全防护网。武汉市网络安全协会党支部书记、专职秘书长刘悦恒出席活动并做分享，桥隧公司党总支委员、一党支部书记杨杭杭主持活动。

2024 年是习近平总书记提出网络强国战略目标 10 周年，是习近平总书记提出总体国家安全观 10 周年。今年的国家网络安全宣传周主题是，网络安全为人民，网络安全靠人民。

活动中，刘悦恒深入讲解了当前网络安全形势和网络安全事件案例，强调了地铁行业作为关键信息基础设施网络安全的重要性和必要性，并分享了防范常见网络攻击、保护个人信息的有效方法。

随后，桥隧公司党员积极参与网安知识问答环节，协会党员向回答正确的同志们颁发网安周宣传纪念品，桥隧公司党员纷纷表示将把网络安全知识融入日常工作中，为保障武汉地铁网络安全贡献力量。

此次 2024 国家网络安全宣传周主题党日活动，不仅提升了桥隧公司党员的网络安全意识，也拓展了武汉市网络安全协会与国企之间的党组织党员合作交流渠道。双方表示，将继续携手前行，共同应对网络安全挑战，为维护国家网络安全作出更大贡献。

2024 武汉市网络安全宣传周
灯光秀绽放两江四岸

2024 年 9 月 9 日至 15 日，国家网络安全宣传周以“网络安全为人民，网络安全靠人民”为主题，在全国展开。武汉积极响应，举办了一系列精彩纷呈的宣传活动，旨在增强市民的网络安全意识。

此间，长江汉江两岸四岸夜景因网络安全主题灯光秀而绚丽夺目。

图 1：龟山电视塔在夜色中巍峨耸立，塔身光影变幻，映出宣传周主题。

图 2：汉口江滩建筑群灯火辉煌，与江面倒影交相辉映，滚动展示着网络安全标语。

图 3：汉口江滩建筑群灯火辉煌，与江面倒影交相辉映，滚动展示着网络安全标语。

图 4：武昌江滩，黄鹤楼与现代建筑群灯光璀璨，在长江水波中相映成趣，将网络安全的信息传递给每一位市民。

市民们驻足观赏，不仅享受了一场视觉盛宴，更在潜移默化中深刻认识到网络安全的重要性。这场灯光秀，让网络安全理念在江城武汉熠熠生辉。

网络安全宣传深入全市基层场所

为进一步扩大网络安全宣传效果，武汉市在 2024 年国家网络安全宣传周期间，充分调动资源，利用全市 4000 余台公安反电诈宣传机，展开了一场深入全市各个基层场所的宣传活动。

在武汉各大医院等公共场所，反电诈宣传机正播放着生动的网络安全宣传视频，吸引了不少市民驻足观看。

地铁站内，人来人往，但公安反电诈宣传机的屏幕依然引人注目。屏幕上，市民正在学习最新的网络诈骗手段和防范措施。

这些宣传机遍布商业街区、办公楼宇、医院、酒店、车站、地铁、博物馆、体育馆等公共场所，实现了宣传的全覆盖和无缝衔接。通过持续播放网络安全宣传视频和海报，极大地提升了宣传的针对性和实效性，让网络安全理念深入人心，共同构建安全、和谐的网络环境。

网络安全宣传主题
卡通人物亮相百年汉口老街

在今年的国家网络安全宣传周期间，在武汉黎黄陂路这一百年汉口老街上，网络安全宣传主题卡通人物文文和安安成为了市民和游客们争相合影的网红打卡点。

黎黄陂路位于江岸区原汉口俄租界区，是武汉的一条历史文化名街。这里不仅保留了丰富的历史遗迹，还巧妙地将武汉传统文化与现代气息相结合，吸引了众多市民和游客前来游览。而文文和安安的亮相，更是为这条老街增添了新的亮点和活力。

此次文文和安安的打卡活动，不仅让市民们在轻松愉快的氛围中学习到了网络安全知识，还提高了大家对网络安全的重视程度。市民们表示，这种宣传方式既新颖又有趣，让人在欣赏美景的同时，也能深刻感受到网络安全的重要性。

文文和安安的亮相和市民深度互动，让我们看到了市民们对网络安全宣传的积极响应和支持，也看到了文文和安安作为网络安全宣传大使的魅力和影响力。相信在未来的日子里，文文和安安将继续陪伴市民们，共同守护网络安全，让这座城市更加美好。

图：市民与文文和安安合影打卡

网络安全宣传周走进湖北大学

2024 年 9 月 9 日至 15 日，国家网络安全宣传周火热开启，“网络安全为人民，网络安全靠人民”的主题响彻全国。武汉市网络安全协会积极响应我市国家网络安全宣传周工作部署，举办了一系列精彩纷呈的活动，其中“走进湖北大学”这场活动更是令人惊艳。

9 月 10 日的湖北大学热闹非凡。网络安全宣传展板摆放得井井有条，展板内容生动有趣，犹如一幅幅漫画，清晰地展示网络安全知识，引得同学们纷纷上前观看。

在“非遗遇见网络安全”趣味活动中，非物质文化遗产与网络安全完美结合。漆扇制作过程仿若一场奇妙派对，让同学们在体验中感受到传统文化与现代科技的碰撞，深刻认识到网络安全的重要性。

图 1：宣传展板前，同学们像小蜜蜂一样围在一起，认真学习网络安全知识

图 2：“非遗遇见网络安全”趣味活动现场，同学们玩得不亦乐乎。

非遗遇见网络安全

9 月 11 日宣传讲座更是座无虚席人气爆棚。武汉市网络安全协会的专家们深入浅出的讲解，同学们听得津津有味，期间互动不断，气氛热烈。此次讲座还邀请了网安龙头企业专家，为大家带来了前沿技术讲座，包括人工智能安全、数据安全、智能网联汽车安全等最前沿的技术和产业动态，都被大咖们一一道来，同学们犹如打开了新世界的大门。

图 3：宣传讲座现场，同学们一个个都像小海绵，拼命吸收着知识。

本次活动不仅吸引了网络空间安全学院的百名师生参与，计算机与信息工程学院、人工智能学院等多个学院的师生也纷纷闻讯赶来。

通过这次活动，湖北大学师生们收获颇丰，学到了丰富的网络安全知识，对前沿技术也有了更深入的了解。它就像一场及时雨，极大地提升了校园的网络安全意识，为打造安全的网络环境奠定了坚实基础。

武汉市网络安全协会“走进湖北大学”活动的成功举办，为 2024 年武汉市国家网络安全宣传周增添了一抹亮丽的色彩。

图 4（花絮）：宣传讲座现场，精彩演讲和互动让他们连连点头

网络安全“童”行 守护数字未来




为响应 2024 年国家网络安全宣传周，9 月 11 日，武汉市网络安全协会联合武汉市硚口区荣华社区走进到硚口区井冈山小学，为青少年们带来一场主题为“网络安全‘童’行 守护数字未来”的宣传课，引导青少年在新学期树立安全健康的上网观念，争做网络好少年。

课堂一开始，老师从“大家平常用网络做什么”“什么是黑客”“什么是计算机病毒”这些青少年们感兴趣的问题出发，结合图片视频，引导青少年正确理解网络安全的内涵和实质，带领学生了解了网络信息诈骗、网络沉迷预防等方面的知识，为了进一步加深网络安全意识，还组织了互动环节，青少年们踊跃举手发言，分享自己对网络的看法，老师耐心解答同学们的疑问，同时通过真实案例的分享，向青少年们传授了保护个人隐私使用技巧，让青少年们深刻认识到网络违法行为的严重性和危害性，引导他们树立正确的网络观念和行为习惯。

最后，青少年们还共同合唱《网络安全拍手歌》，在愉快的歌声中结束了这堂意义匪浅的网络安全教育课，青少年们纷纷表示要自觉抵制网络不良信息，保护个人信息安全，争做网络安全小卫士。

本次活动支持单位：湖北东方网盾信息安全技术有限公司


网络安全宣传周
共筑安全防线走进人保武汉分公司

线上 + 线下活动现场

武汉人保副总经理苏彦红发表致辞

武汉市网络安全协会网安保险专委会秘书长周韬发言

武汉大学国家网络安全学院于博洋博士精彩演讲

武汉人保东西湖支公司的张琪带来关于网络安全保险的专业培训

在 2024 年国家网络安全宣传周的大背景下，武汉人保于 9 月 12 日迎来了一场意义深远的“网络安全走进人保，共筑安全防线”活动。这一活动在中国人民保险武汉分公司举行，备受瞩目。

此次活动由人保武汉分公司与武汉市网络安全协会联合主办。为了让更多人参与其中，活动采用了线上与线下相结合的多元模式。在活动现场，众多保险行业的从业者们纷至沓来，齐聚一堂。

活动期间，大家积极参与讨论，致力于提升网络安全意识。

网络安全在当今社会至关重要，尤其对于保险行业而言，它关系到客户信息的安全以及业务的稳定运行。参与者们围绕网络安全在保险行业中的应用与实践展开了深入且细致的探讨，涵盖了如何防范网络攻击、保障数据安全等诸多关键领域，为保险行业的网络安全发展注入了新的活力。

优秀工作者丨李玲
——新时代我省网安职业高技能人才培养的践行者

2022 年 10 月，中共中央办公厅、国务院办公厅发布《关于加强新时代高技能人才队伍建设的意见》，为新时代高技能人才队伍建设擘画了新蓝图。意见中明确提出要加强高级工以上的高技能人才队伍建设；加大高技能人才培养力度；建立技能人才职业技能等级制度和多元化评价机制。

在网络强国的大背景下，李玲作为武汉安域信息安全技术有限公司（以下简称“武汉安域信息”）培训部负责人，自 2018 年起就扎根于国家网络安全人才与创新基地，从参与网安基地建设到聚焦于网安职业技

能人才培养，李玲始终坚持在网安人才培养道路上砥砺前行。

一、开展网安实战型人才培养课题研究

能源安全是国家安全的重要组成部分，是国家战略安全和经济社会发展的基础保障，是关系国计民生、国家安全的重要关键信息基础设施，同时也是技术、资金密集型行业，能源领域网络安全人才培养工作是能源安全的重要保障。但是，我国能源领域网安人才整体数量不足、跨领域能力不够、实战能力欠缺、发展不均衡不充分等问题较为突出，难以满足能源领域关基背景下对网安人才的要求。

为加快推进能源领域网络安全实战型人才培养工作，武汉安域信息依托在能源行业的网络安全技术、培训能力及生态体系优势，承接了武汉市能源领域《网络安全实战型人才培养指南》的课题研究。李玲作为该课题负责人，重点从行业调研、指导小组及编制小组筹建、编制计划的制定和把控、创新性和先进性保障、质量保障等方面下大功夫，组织编制小组从运营体系建设、课程建设标准及大纲内容、师资标准及师资库建设、电力工控实训平台建设标准、培训考核体系建设等方面出色完成了课题研究工作，为我市能源领域网络安全实战型人才培养工作贡献了有利支撑。

二、重点参与关保培训基地能力建设

2023 年 11 月 1 日，中央网信办正式授予国家网络安全人才与创新基地为“国家关键信息基础设施安全保护培训基地”。武汉安域信息承接了国家关保培训基地之能源行业的五项能力建设，包括教材编写、师资库建设、课程开发、实训平台建设及考核体系建设。李玲作为该项国家级课题的负责人，组建了一支层次分明、结构合理、具备行业代表性的项目专家队伍。她带领项目团队深入电力、煤炭、天然气、石油等单位进行人才现状调研，采集了重点领域人才需求的关键信息，整个课题聚焦重点行业、关键岗位人员职业技能实战能力提升，高质量完成了课题结项。

三、积极投身湖北省网安高技能人才培养事业

近年来，国家人社部门联合相关主管部门，相继发布了网络安全相关职业及各职业技能标准，大力推动网络安全职业技能人才培养及评价工作。武汉安域信息聚焦湖北省“51020”现代产业体系及武汉市“965”产业集群发展，助力人才引领驱动发展，打造新质人才生产力发展高地。李玲作为公司人才培养战役的主帅，带领战役小组扎实推进和落实高技能人才培养能力建设、认定资质申报及运营、一线工作开展。2023 年面向来自于高校科研机构、安全厂商、培训机构、安全服务集成商等近一百余名申报者，开展了网络安全相关的一级 / 高级技师、二级 / 技师认定工作。2024 年，在湖北省密码管理局及湖北省商用密码协会的指导下、战略合作单位的共同支持下，李玲和公司的技术总监柳少凯共同带领团队在国家网安基地建设完成了“商用密码行业技术应用实验室”项目，包括商用密码实训平台建设、行业技术应用优秀解决方案展示、商用密码应用安全性测评实验环境建设、密码技术应用员培训能力及认定能力建设。自 2024 年下半年起，已持续面向社会从业人员开展密码技术应用员三级 / 高级工、四级 / 中级工的培训及认定工作，为湖北省商用密码事业发展贡献人才力量。

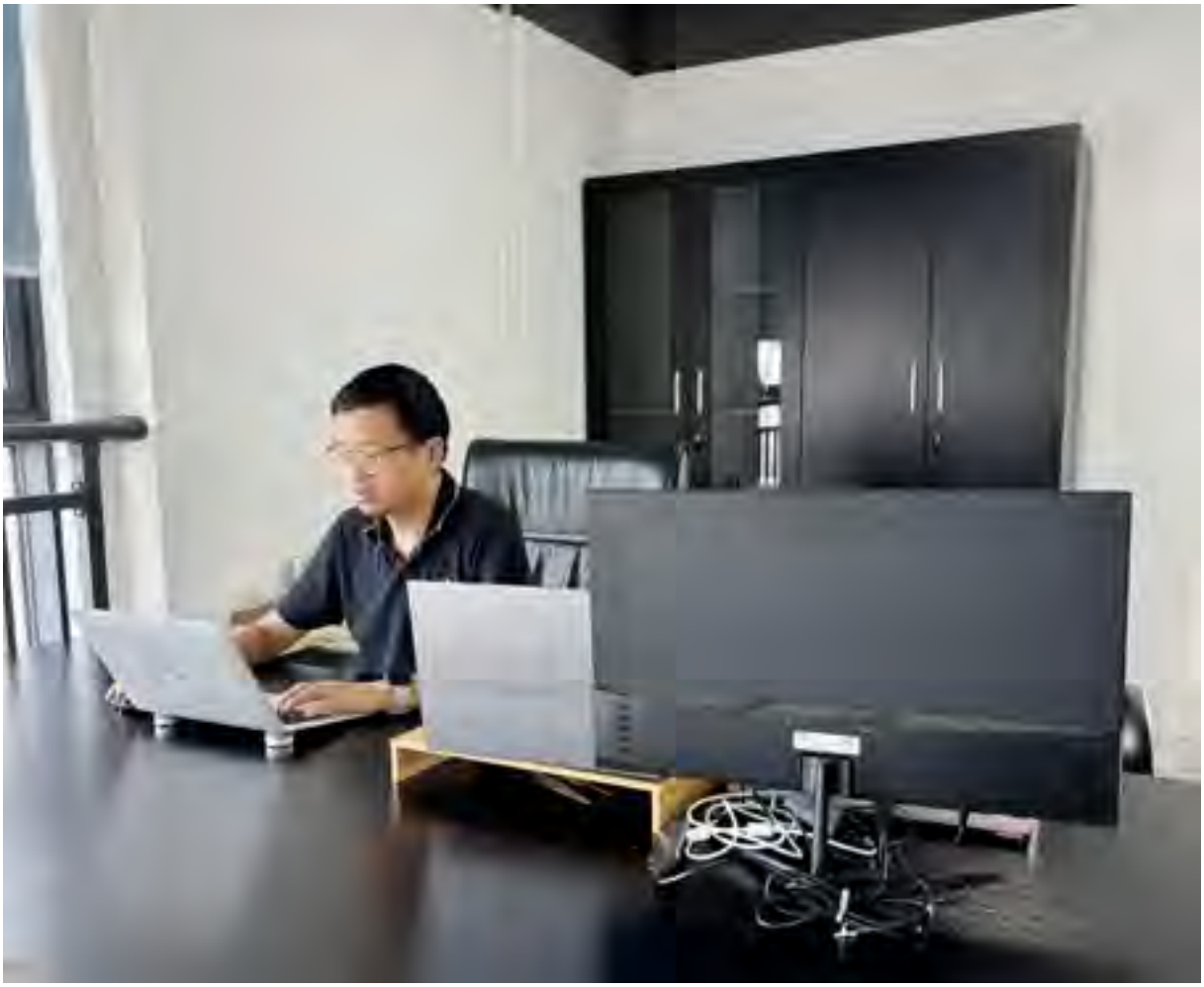
四、深度参与协会各项培训赛事活动

为了专业化、体系化、常态化推进我市网络安全人才培养工作，协会于前年成立了培训中心，并由李玲担任培训中心主任，主要负责围绕武汉市网信中心的工作，提供高质量的培训赛事工作支撑。在过去的一年时间，她重点参与了协会人才专委会的筹建、数项重要培训赛事活动的筹备和实施、国家网安周公益活动，为协会的高质量发展提供了切实支持。

网络空间的竞争归根结底是人才的竞争，李玲用实际行动积极践行“非为已往，非为现在，而专为将来”的家国大任。她表示未来将持续坚守在网络安全人才培养的岗位一线，为网安国安贡献微薄之力。

（供稿：武汉安域 袁甜）

优秀工作者丨雷彦章
——守护网络，细节见证非凡



在这个信息高速流转的时代，网络安全已成为举足轻重的大事。在这样一个容不得半点差错的领域，有一位不为人知的英雄，他的名字叫雷彦章。一位普通的网络安全工程师，却以他的专业和坚守，为网络世界筑起了一道道坚固的防线。

雷彦章的日常工作，表面看来平平无奇，但正是这种看似平凡的工作，却包含着不平凡的贡献和意义。每一天，当大多数人还在沉睡中，他已经出现在自己的工位上。他的桌子上摆放得井然有序，每一张纸张、每一个文件夹，都分类得整整齐齐。他认为，做好网络安全工作，首先要从自己的工作环境做起，这不仅是对自己职责的尊重，也是对工作效率的追求。

对雷彦章来说，每一行代码都有它自己的语言和意义，每一个数据包都可能隐藏着潜在的威胁。在他的眼中，这些不是单调乏味的字符，而是需要深入解读的信息。他的闪光点在于，他坚信即使最微小的异

常也不可忽视，这种专注的精神让他在常人难以察觉的细节中，发现并阻止了无数次网络攻击。

他的感人之处在于那股不服输的韧性。记得有一次，公司服务器遭遇了复杂的网络攻击，许多同事都感到束手无策，但雷彦章却挺身而出，连续工作了 36 个小时，最终找到了缓解攻击的方法。他总是这样，用实际行动诠释什么是真正的专业精神和艰苦奋斗。

在同事眼中，雷彦章是个温和而又认真的人。他总是乐于助人，对待新员工更是耐心十足。记得新来的张强，刚接触网络安全不久，对于复杂的系统感到十分苦恼。是雷彦章在工作之余，不厌其烦地为他解答问题，甚至牺牲自己的休息时间，帮助他逐渐熟悉工作流程。正是这种细微之处的关怀，让团队的氛围更加和谐，也让每一个成员都感受到了集体的温暖。

雷彦章最可贵的，是那种不求回报的敬业精神。即使是在周末或假日期间，只要公司的系统出现了任何问题，他总是第一时间出现在办公室，毫不犹豫地投入到解决问题中去。他深知，网络安全的每一秒钟都至关重要，他的坚守，可能就是保护成千上万人数据安全的关键。

如今，雷彦章已经在网络安全领域工作了十多年。这十多年，他从一名青涩的新人成长为团队的中坚力量。面对日益严峻的网络安全形势，他始终保持着一颗学习的心，不断更新自己的知识体系，跟上时代的步伐。

除了承担繁重的日常工作，雷彦章还积极参加各种网络安全会议和培训。他深知，只有不断地学习和进步，才能应对不断变化的安全威胁。同时，他还积极参与行业内的技术交流，与同行们分享经验和心得，提升整个行业的安全防护水平。

雷彦章的职业生涯不仅充满了挑战，也充满了成就感。他曾多次参与解决重大安全事件，获得了公司高层的高度认可。然而，他从不居功自傲，而是把每一次成功当作新的起点。他常说：“网络安全没有终点，只有不断前行。”

雷彦章，这个名字或许不会出现在报纸的头条，也不会有人为他颁发奖章。但在需要他的地方，总能看见他忙碌的身影。他的故事，证明了一个真理：英雄不仅存在于战场，还存在于我们每个人身边。他用自己的行动诠释了什么是责任，什么是奉献。

雷彦章的故事，虽不轰轰烈烈，却让我们明白，每一个平凡岗位上的工作者，都有可能成为不平凡的英雄。他们是这个时代最美的风景，也是网络世界宁静与安全的守护者。他的故事，是对每一个网络安全工作者的最好致敬，他的精神，值得我们每一个人学习和传扬。

（供稿人：曙光网络 杨琛）

优秀工作者 | 汪天武
——铸就数字时代的铜墙铁壁

在数字浪潮汹涌澎湃的今天，网络安全已不再是简单的技术挑战，而是关乎国家安全、经济命脉和社会稳定的重大议题。在这片复杂多变的网络疆域中，汪天武，一位网络安全领域的精英，以其深厚的专业素养、不懈的创新精神和无私的奉献精神，成为了守护数字时代网络安全的坚固盾牌。

一、坚守网络安全使命和责任

2015 年选择信息安全专业是汪天武踏上网络安全这条路的开始，至此，他便始终谨记网络安全不仅仅是技术的较量，更是责任与使命的担当。2019 年军运会，他作为迪普科技在武汉的项目实施经理，统筹协调多个单位的网络安全防护工作，军运会期间成功守护武汉网络安全环境。在进行网络安全工作的同时，他也意识到日益严峻的网络威胁，深感自己肩负的责任重大。这份责任感，驱使着他不断深入研究，力求在网络安全领域取得突破。

二、坚持学习、不断创新

网络安全技术的快速发展，既带来了前所未有的机遇，也伴随着层出不穷的挑战。汪天武深知，只有不断创新，才能在这场没有硝烟的战争中占据主动。他多次参数湖北省各大安全活动，例如各单位组织的攻防演练，省护网，安全圈子活动，ctf 比赛等，通过不断的学习交流，实战攻防来加强自己各方面的网络安全能力。

网络安全是一场实战性极强的战斗。汪天武深知，只有经历过实战的洗礼，才能真正成长为一名优秀的网络安全工作者。他多次参与湖北省各单位重大活动的网络安全保障工作，面对复杂多变的网络环境和突如其来的网络攻击，他总能迅速反应，准确判断，有效应对。

这些宝贵的实战经验，不仅锤炼了他的专业技能和心理素质，更为他日后的工作奠定了坚实的基础。

三、分享 & 贡献

汪天武深知，网络安全事业的持续发展离不开人才的支撑。因此，他积极投身于网络安全教育和人才培养工作。他在武汉某高校提供网络安全课程指导，传授最新的安全技术和理念；他希望通过自己的努力，能够激发更多年轻人对网络安全的兴趣和热情，为网络安全事业培养更多的优秀人才。

汪天武的故事，是无数网络安全工作者奋斗历程的缩影。他们用自己的智慧和汗水，维护网络安全世界的安宁与稳定。在这个充满挑战与机遇的时代，让我们以汪天武为榜样，不忘初心，牢记使命，不断追求卓越和创新，共同铸就数字时代的铜墙铁壁，为构建网络强国贡献自己的力量。

（供稿人：迪普科技 曹思炜）

优秀工作者｜李航
——不断探索，砥砺前行

李航，男，1993 年出生，湖北宜城人，毕业于武汉理工大学，计算机科学与技术专业。曾响应国家号召，参军入伍成为一名光荣的武警战士，在校和服役期间，他不断加强学习，将自己的爱好转化为自己前进的动力，不断深入网络通信、网络安全方面的研究。

网络安全，一个关乎国家安全、企业利益、个人隐私的重要领域，需要有一群默默无闻的守护者，在这群守护者中，李航同志以其卓越的技能、深厚的理论知识和丰富的实践经验，成为了我公司网络安全领军人物。

李航同志一直以来在北京、武汉等地辗转学习多年，为各企业的网络安全做出了卓越贡献，他曾成功在国家级攻防演练中，成功防御了来自各地黑客的攻击，并成功溯源黑客，被单位评为“先进个人”，保障了企业的网络安全。

在企业工作期间，也曾受省经信委委托企业对全省工业规模以上企业，进行网络安全检查，检查中帮助企业发现并处理高危网络安全问题，及时排除了企业被勒索的隐患。

除了应对突发事件，他在蓝芽网络日常工作中也展现了极高的专业素养，他深入了解各种网络安全攻击手法，不断更新和完善防御策略，他还参加各类 CTF 比赛，锻炼自己技术能力。在连续三年的国家级攻防演练行动中，通过积累的网络安全经验，精准布防，精准溯源，帮助某央企拿下网络安全攻防演练先进单位及各类 CTF 比赛奖项。

更为难能可贵的是，他始终保持着对技术的热爱和追求，在取得部分成绩的同时，他也没有停下脚步，仍然保持着对新技术的探索和研究。他的这种精神，感染和激励着周围的同事。

当然，网络安全并不是一蹴而就的事情，需要全社会的公共参与和努力，李航深知这一点，他经常在企业和高校进行网络安全意识培训，普及网络安全知识，提高大家的网络安全意识，在他的影响下，公司所负责的大、小企业均达到了网络安全“零事件”。

如今，他依然坚守在网络安全的第一线，用自己的智慧和力量守护着心中的信念，为网络安全事业贡献自己的力量。

（供稿人：蓝芽网络 余芳）

优秀工作者｜管鹏飞
——坚守网络安全防线，十年不凡之路

从事网络安全工作超过十年的管鹏飞，给人的第一印象是沉稳而内敛。然而，在他平静的外表下，却隐藏着一颗对网络安全事业无比炽热的心。这份热爱，源于他对网络世界深深的责任感。

十年前，管鹏飞踏入了网络安全领域，成为了一名普通的网络安全工程师。那时候的他，怀揣着对技术的热爱和对未来的憧憬，踏上了这条充满挑战的道路。十年后，他成为了这个领域的领军人物，带领着他的团队在网络安全的大潮中乘风破浪。

他的工作看似平凡，却处处闪耀着不平凡的光芒。他深知网络安全的重要性，每一次攻防演练，每一次漏洞排查，他都亲力亲为，不容有失。在他的带领下，珞格科技团队多次成功抵御了网络攻击，保障了客户数据的安全。这些成绩的背后，是管鹏飞对网络安全事业的无限热爱和对技术创新的不懈追求。

他的感人之处，更在于他对待工作的那份执着和坚守。网络安全工作是一项需要长期投入、持续努力的事业。在这个过程中，管鹏飞一直保持着高度的责任心和使命感。无论面对何种困难和挑战，他都能坚持到底，从不轻言放弃。这种精神，不仅激励着他自己在网络安全领域不断前行，也感染着身边的每一个人。

在常情之中，管鹏飞的可贵之处更是显而易见。他对待同事如家人般温暖，总是耐心倾听他们的想法和困难，给予最大的支持和帮助。在他的带领下，珞格科技团队形成了一股强大的凝聚力和战斗力。这种团队精神，也成为了珞格科技在网络安全领域不断前行的强大动力。

他的事迹不仅仅是在网络安全行业内的先进典型，更是一种精神的感召。他用自己的实际行动诠释了什么是责任、什么是担当。在他的身上，我们看到了一

个网络安全人的坚守和执着，也看到了一个科技企业的社会责任和担当。

正是因为有了像管鹏飞这样的守护者，我们的网络世界才能更加安全、稳定。他的故事激励着更多的年轻人投身网络安全事业，为构建更加美好的网络空间贡献自己的力量。

管鹏飞常说：“网络安全无小事，每一个细节都不能忽视。”这句话不仅是他工作的座右铭，更是他生活的写照。他用自己的平凡之躯，筑起了一道不平凡的网络安全防线。在这个充满挑战和机遇的时代，我们需要更多像管鹏飞这样的人，用他们的智慧和勇气，守护我们的网络世界。

展望未来，他和他的团队将继续在网络安全领域深耕细作，不断创新、不断进步。他们相信，只要心中有光、脚下有路，就一定能够走出一条属于自己的网络安全之路。让我们期待他们在未来的网络安全事业中创造更多的辉煌！

（供稿人：湖北珞格 乔路）

优秀工作者｜周阳波
——树智网之魂、铸网安之盾

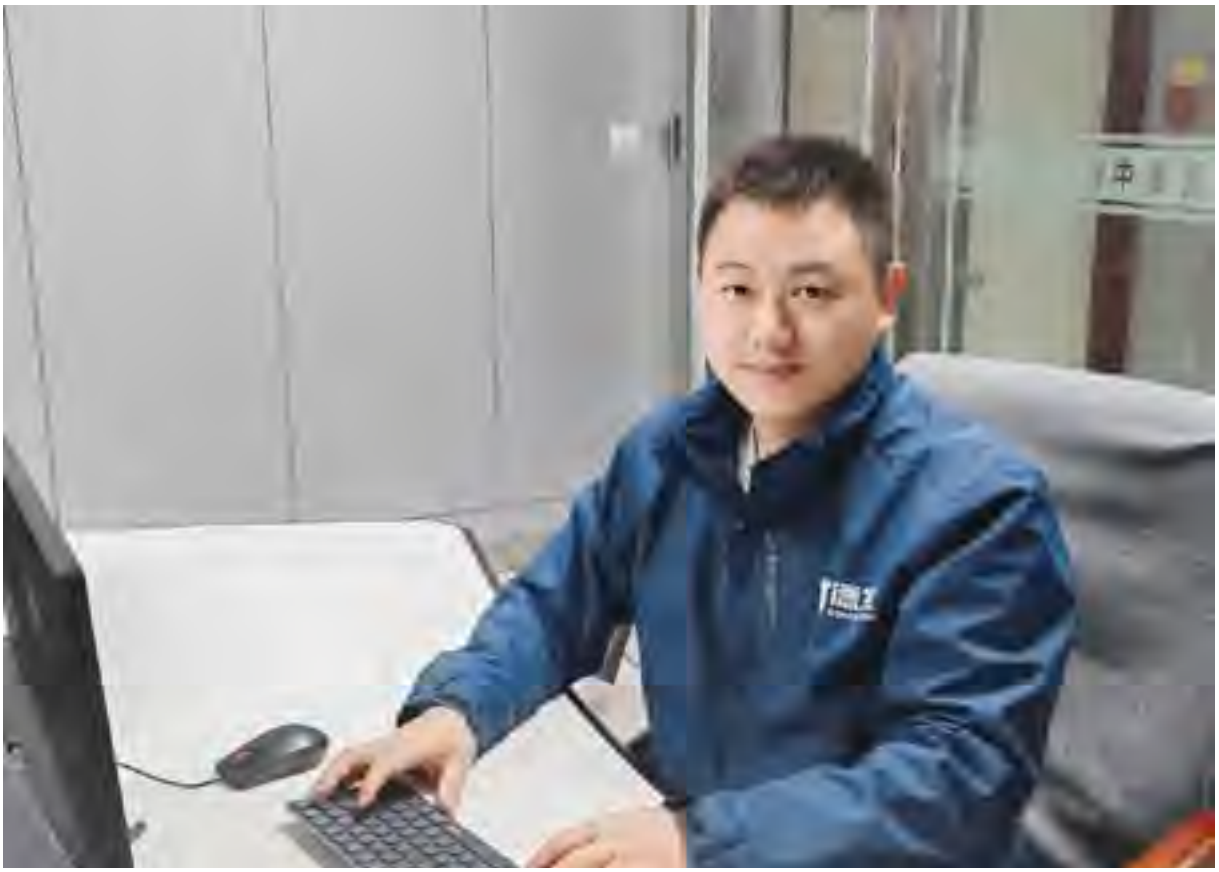
作为一名资深的网络安全专家，周阳波同志深知网络安全对于国家、企业和个人至关重要。他带领管理团队攻坚克难、努力创新，致力于提高公司的技术水平和创新能力。公司在近几年快速发展中，不断推出领先行业的产品和服务，获得了业界多项荣誉，为客户的网络安全保驾护航做出了卓越成绩。

作为一家成长性旺盛的高新技术企业，智网安云在该同志的带领下，在武汉市乃至全国的网络安全行业形成了较大影响，使得智网安云目前在武汉市快速成长为一个专业资质最全、提供网络安全技术支撑最专业的企业。目前公司已经拥有 13 项专利、软著 43 项、超过 30 项原创漏洞证明等。智网安云公司还拥有湖北省专精特新“小巨人”企业、第一批入库湖北省科创“新物种”瞪羚企业、湖北省上市后备“银种子”企业等称号。另外，公司还入选 2022 年工信部大数据产业发展试点示范项目名单、2024 年度工业信息安全监测应急支撑单位等多项荣誉。

在产学研方面，他带领着管理团队积极与各大高校进行深度合作。目前智网安云已经与澳门城市大学、西安电子科技大学等高校建立联合实验室，致力于共同研发新技术、新产品推动国家网络安全行业的快速发展。

周阳波同志积极履行社会责任。作为武汉工商联执行委员、东西湖区工商联执行委员，他身兼多职积极参与各种公益活动，为提高全民网络安全意识贡献自己的力量。

优秀工作者丨李勇
——筑牢数字长城：网络安全卫士的坚守与奉献



李勇的故事是网络安全领域内众多默默奉献者的一个缩影，同时也是武汉德发公司 IT 运维团队中一颗璀璨的明星。作为德发公司的一名运维管理者与资深 IT 工程师，他的经历生动诠释了网络安全工程师这一职业的责任感与使命感。从计算机专业的学习到投身德发公司的网络通信运维，再到专注于网络安全，李勇的职业路径不仅展现了他对网络安全的深刻理解与不懈追求，也深刻体现了德发公司在培养技术人才、应对网络安全挑战方面的坚定决心和实际行动。

在负责的网络运维日常工作中，李勇面临着一个尤为棘手的挑战：所维护的某政府单位网络环境既复杂又至关重要，却频繁地遭受着各式各样的网络攻击。当时，该单位暂未配备专门的网络安全工程师，而德发 IT 运维团队作为客户的技术支持方，也亟需帮助客户解决这一紧迫问题。面对这一挑战，李勇没有选择逃避，而是毅然决然地承担起了这份重任，成为了德发公司在网络安全领域的先锋。

他利用宝贵的业余时间，犹如海绵吸水般恶补网络

安全知识，同时充分利用德发公司提供的资源和平台，深入学习并实践网络安全技术。在短短三个月的时间里，他通过自学与实践的紧密结合，以及德发公司团队的支持，成功攻克了客户的网络安全难题。这一过程中，他不仅深刻领悟到了网络安全的重要性，更在解决问题的过程中体验到了前所未有的成就感，也为德发公司在网络安全领域树立了良好的口碑。

然而，对于李勇而言，这仅仅是个开始。他深知网络安全领域的变化与发展日新月异，需要不断地学习与更新知识才能跟上时代的步伐。因此，他继续在业余时间深入研究网络安全的最新技术和趋势，努力提升自己的专业素养。在他的不懈努力下，该单位终于建立起了一套完善的网络安全防护体系，有效地抵御了网络攻击的威胁，也为德发公司赢得了客户的信任和赞誉。

李勇的领导力和敬业精神在德发公司的网络安全工作中得到了淋漓尽致的展现。他以身作则，带领团队日复一日地检查网络设备、分析安全日志、升级安全策略。这些琐碎而重要的工作在他的带领下变得井然有序，德发公司的网络安全水平也因此得到了显著提升。他深知，每一次成功预防潜在风险，都是对团队辛勤付出的最好回报，也是对自己和德发公司职责的最好诠释。

此外，他还充分利用空余时间，带领团队参加“楚慧杯”网络安全大赛，参与 CISAW（信息安全保障人员）培训并通过认证。这些活动不仅提升了团队的整体实力和战斗力，也为德发公司在网络安全领域树立了更高的地位和影响力。在他的带领下，团队成员们团结一心，共同为网络安全事业贡献着自己的力量。

有人说，网络安全工程师是网络世界的守门人，他们默默守护着网络空间的安全，以辛勤的付出换得了亿万用户的安宁。李勇的故事，无疑为我们展现了一个立体而饱满的网络安全工程师形象，同时也让我们看到了德发公司在网络安全领域的坚定决心和实际行动。

在这个充满挑战与机遇的网络安全领域里，有着许多像李勇这样平凡而又不平凡的人，他们都在各自的岗位上默默守护着网络空间的安全。虽然他们的名字未必广为人知，但他们的努力与奉献无疑是对国家、社会、人民最大的贡献。让我们向这些隐形英雄致以最崇高的敬意，感谢他们为网络安全所做的一切。他们是我们网络安全的重要保障，也是我们社会进步的重要推动力量。在他们的引领下，我们有信心应对任何网络安全挑战，也有决心构建一个更加安全、繁荣的网络空间。而武汉德发公司，作为这些英雄们的坚强后盾，也将继续为网络安全事业贡献自己的力量，共同守护我们的数字世界。

（供稿人：德发电子 王晓）

优秀工作者丨刘培培
——信息化服务行业的守护者

在繁忙的信息化服务行业中，有一位人物凭借其不凡的坚守和卓越的表现，成为了行业中的一道亮丽风景线。他，就是我们所要讲述的主人公，一位名叫刘培培的信息化服务者。

刘培培的工作日常并不轰轰烈烈，甚至可以说是平凡。然而，就在这份平凡之中，他发现了自己的“闪光点”，那就是对每一个细节的极致追求和对工作的无限热爱。他深知，信息化服务工作需要耐心和细致，需要不断地学习和探索。因此，他始终保持着对新技术、新知识的渴望，不断提升自己的专业素养。

国家网络安全宣传周，武汉同德兴公司的刘培培积极配合武汉市网络安全协会举行了一周的武汉国家网络安全宣传周进校园公益活动，在武汉市光谷第十六小学、武汉市博学小学、新洲区邾城街中心小学、武汉市第六十四中学、新洲区实验中学及武汉光谷外国语学校给全体师生宣讲，活动主题为”争做网络安全小卫

士”，期间以有趣的互问互答形式来讲述网络的优缺点，让学生结合实际讲述自己的观点，共讲述了三个关于网络危害的案例来引起学生对网络安全的重视，告诫学生注意网络信息安全，提高自我防范意识，教了四个网上自我保护的方法，最后还有一些随堂小测试来增加学生记忆点。此次活动同德兴积极投身到投身武汉市网络安全宣传工作中让学生师生认识到了维护网络安全不仅是国家的事情，而是大家小家千万家的事情，人人都要为此贡献出一份自己的力量，来共同维护我们这个”大家”，一起勇担社会责任。

刘培培的闪光点不仅在于他的专业技能，更在于他的人情味和责任心。在与客户沟通时，他总是能够敏锐地洞察到对方的需求，提供贴心、专业的服务。在团队中，他乐于助人、甘于奉献，成为了同事们信赖和依靠的对象。正是这种人情味和责任心，让刘培培在细微之处找到了“感人点”，也让他的工作成果更加出色。

当然，刘培培的可贵之处还远不止于此。在信息化服务行业中，安全问题始终是重中之重。而刘培培正是凭借着对安全的深刻理解和不懈追求，从常情之中挖掘出了“可贵点”。他不仅注重技术层面的安全防护，更关注安全意识的普及和提升。他经常组织安全培训和演练，提高团队成员的安全意识和应对能力。正是这种对安全的执着和坚守，让刘培培成为了网安行业的先进典型。

在今后的日子里，他将继续坚守自己的岗位，为信息化服务行业的发展贡献力量。而我们也有理由相信，在他的带领下，更多的优秀人才将涌现出来，共同推动整个行业不断向前发展。

优秀工作者丨方浩
——“网”上强人 “线”上精英

方浩，如静水流深，技术精湛；如磐石坚定，责任心强。在数字世界的脉络中，他以匠心守护网络安宁，确保网络业务系统的安全稳定。

1、精心组织，保障关键基础信息设施安全稳定运行

金税四期数字电子发票平台的上线，标志着税务管理数字化、智能化的重大突破。在 2023 年 4 月 17 日至 8 月中旬的关键时期，省级税务局精心部署并逐步推进了数字电子发票平台系统的上线工作。

项目伊始，团队针对网络应用逻辑区域进行了精细的安全域划分，并专注于安全设备的安装调试与测试工作，这是为了构建一个坚不可摧的网络安全立体防线，确保各项应用的安全性和可靠性。随后，技术团队稳步推进应用软件的基础环境搭建，为系统提供了一个稳固的技术支撑平台。在系统即将上线前，由他带领的网络安全团队，对系统进行多次模拟攻击测试和安全隐患的扫描发现，最终制定并实施一系列安全防护策略，这些策略的配置实施有效地实现了云外系统与云内系统的安全互通，从而保障了数据传输的安全性和流畅性。为金税四期数字电子发票系统提供了一个安全、稳定、高效的网络基础平台。

2、强化宣传培训，提升社会网络安全防范意识

除了在网络安全技术方面的钻研外，他还在网络安全防范意识上积极行动，走进武汉市江岸区某小学校园，引导学生绿色上网并利用好网络帮助教学；走进政府机关和企事业单位，他结合国内外网络安全形势，从不法分子网络入侵途径、网络安全常见误区、如何提升网络安全意识等方面，深入浅出地阐述了网络安全工作的重要性，为政府机关和企事业单位网络安全建设提供了大量的咨询与建议。

3、带领团队，做好网络安全守护者

作为网络安全团队负责人，更是展现了较强的领导力和模范带头精神。他带头钻研网络安全技术，先后考取了信息系统项目管理师、CISP-PTS 等证书，不仅是团队中的技术楷模，更是心灵的导师。在他的鼓励和指导下，团队成员不断超越自我，在各自擅长的领域深钻技术，实现了个人的成长与团队的和谐共进。一直以来所倡导的团队内部开放沟通和技术知识共享文化，已经深深植根于团队的基因之中。

他所带领的技术团队具备深厚的专业知识和精湛的技术能力，成功实施部署了一系列网络安全防护体系，不仅提高了客户单位网络系统的稳定性和安全性，还大大增强了数据处理能力和用户体验。这些成就的背后，是他在实际工作中不断总结和思考，是他细致入微的项目管理能力与前瞻性的技术洞察。

面对网络威胁和安全挑战，他始终如一地保持着冷静与专注。他不仅及时成功应对了多起网络安全事件，还主动出击，不断钻研新的安全防护技术，并应用于用户的安全防护体系中，为用户单位筑起了一道道坚不可摧的安全屏障，有力地保障了用户单位网络安全稳定运行及数据的安全完整性。

（供稿人：湖北中网李珍桢）

优秀工作者 | 蔡松强
——守护网络，捍卫安全

在数字化时代，网络空间成为了国家安全的新战场。在这里，有一群默默无闻的战士，他们用键盘和鼠标保卫着国家的信息安全。他们或许没有显赫的名号，也没有聚光灯的追随，但他们是网络世界的守护者——网络安全工程师。蔡松强，就是这样一位普通的网络安全工程师，他以坚定的意志和专业的技能，守护着网络的安宁。

蔡松强，1994 年出生，目前担任亚信科技（成都）有限公司（以下简称“亚信安全”）的售前工程师。他还是湖北省政府采购专家库、湖北联投集团有限公司等平台的专家。蔡松强拥有软考高级信息系统项目管理师、系统集成项目管理工程师、网络工程师、数据库工程师、注册信息安全专业人员（CISP）、信息安全保障人员认证证书 CISAW（web 安全专业级）、网络安全应急响应工程师证书（CSERE）以及 CNVD 原创漏洞证书等多项专业资质。

2023 年 10 月 2 日凌晨，当大多数人还在国庆假期的梦乡中时，武汉市某学院的网站遭受了攻击，页面被恶意篡改。亚信安全受武汉市公安局网络安全保卫支队的委托，迅速派遣蔡松强前往现场进行应急处置。

蔡松强到达现场后，立即展开了对受攻击服务器的溯源分析。凭借他精湛的技术能力和敏锐的洞察力，经过数小时的细致工作，成功还原了攻击路径。攻击者利用境外 IP 地址（91.90.xxx.xxx）作为跳板，通过高校一个老旧系统的弱口令漏洞，获取了 WordPress 后台管理权限，进而植入病毒木马，夺取了服务器的管理员权限。

进一步分析显示，攻击者早在 9 月 27 日就已获得管理员权限，直到 10 月 2 日凌晨才发动攻击，篡改网站页面，散布恶意言论，企图破坏社会稳定。蔡松强的迅速反应和高效工作，将此次安全事件的影响降到了最低，确保了国庆期间我市网络安全的稳定，赢得了公安网安部门和教育部门的高度评价。

蔡松强始终保持谦逊和低调，他深知网络安全工作的重要性，经常提醒自己和同行，要对不安全和不规范的行为保持警惕，勇于说“不”。他以身作则，积极帮助客户发现、提出并解决问题，将安全工作做在前面，避免事后补救。

在这个信息化飞速发展的时代，我们迫切需要更多像蔡松强这样的网络安全工程师。他们用专业的技能和无畏的精神，捍卫着网络安全，为我们营造了一个更加安全、和谐的网络环境。

（供稿：亚信安全 周冰清）

我会两项团体标准列入 2024 年度武汉市地方标准制修订项目计划

原标题：市市场监管局关于下达 2024 年度武汉市地方标准制修订项目计划的通知

各有关单位：

为贯彻落实《国家标准化发展纲要》和省人民政府《贯彻落实＜国家标准化发展纲要＞的实施意见》，有效推进《加快推动武汉市经济社会高质量发展标准化专项行动计划（2023-2025 年）》，统筹全市农业、工业、服务业和社会事业等领域武汉标准体系建设，提高我市标准供给质量，充分发挥标准对经济社会高质量发展基础性、引领性作用，经前期项目征集、征求市相关行业主管部门意见、组织专家立项论证和网上公示，现确定《秋冬萝卜绿色栽培技术规程》等 46 个制定项目和《燃气管道设施安全保护规程》等 4 个修订项目列入 2024 年度武汉市地方标准制修订项目计划（见附件）。

各行业主管部门和项目承担单位应按照《武汉市地方标准制修订管理办法》的规定，及时组织相关技术人员组成标准起草工作组，确保标准适用性、协调性和一致性，严格技术审查程序，注重标准实施推广，按期高质量完成项目计划。

咨询电话：武汉市市场监管局标准化处，85333554；武汉市标准化研究院标准研究应用中心，83659556。

武汉市市场监督管理局

2024年7月29日

我会赴湖北省团体标准化发展联盟秘书处调研交流

近日，武汉市网络安全协会秘书长刘悦恒、标准化部主任乔奇前往省标准化院及省标准化联盟秘书处，就网络安全和信息安全标准化建设及合作进行了调研交流。

联盟负责人兰铎介绍了标准化服务和质量提升情况。我会刘秘书长表示，将加大双方合作范围，共同推动行业规范、探索网络安全技术创新发展。

会后，湖北省团体标准化发展联盟质量负责人兰铎代表秘书处为我会授予了湖北省团体标准化发展联盟理事单位的牌匾。

标创公司标准化工程师及市场部相关人员参与了此次交流。

《数据要素场内流通安全评估规范》正式发布


团 体 标 准

数据要素场内流通安全评估规范

近日，由武汉安恒信息科技有限公司、武汉市网络安全协会、汉阳区大数据中心、长江水利委员会水文局、武汉大学国家网络安全学院、中国长江电力股份有限公司、湖北数据集团有限公司、武汉数据集团有限公司、武汉市房产和工程建设智能发展中心、武汉网络安全技术有限公司、武汉趣链数字科技有限公司、武当云谷大数据科技有限公司、国网湖北省电力有限公司信息通信公司、湖北华中电力科技开发有限责任公司共同起草的《数据要素场内流通安全评估规范》在全国团体标准信息平台正式发布。

该标准明确规定了场内流通过程中，针对流通主体、流通数据和流通行为进行安全评估的基本要求，旨在为场内流通各方在确保场内流通活动安全开展时进行自评估，或委托第三方专业机构开展数据交易安全评估提供依据，同时也能作为相关监管部门、行业主管部门评价数据流通交易活动安全保障义务履行状况的重要参考，将有力推动数据要素场内流通的规范化与安全化进程，对数据要素市场的健康稳定发展有着极为重要的意义。

《智慧园区网络安全防御体系建设指南》正式发布


团　　体　　标　　准

T/WHCSSA 004—2024

智慧园区网络安全防御体系
建设指南

Guide to the Construction of Smart Park
Network Security Defense System

2024-11-26 发布　　2025-1-1 实施

武汉市网络安全协会　发布

近日，由武汉市网络安全协会、智网安云（武汉）信息技术有限公司、华中师范大学、湖北大学等多所高校、企业及机构共同起草的《智慧园区网络安全防御体系建设指南》在全国团体标准信息平台重磅发布。

智慧园区企业的数字化和网络环境愈加复杂化，网络恶意攻击更加专业化和产业化，入侵手法也愈发多样化与复杂化，使得传统网络安全解决方案不断受到挑战。传统边界防护设备在防御常见威胁上起到了重要作用，但不能防范所有的、新型的攻击行为，包括来自内部和外部的攻击行为，智慧园区面临网络安全威胁的风险逐步增大。

本标准的发布为智慧园区网络安全防御指引方向。它聚焦智慧园区场景，针对共性安全防护目标精心制定了通用的安全防御体系建设指南。这将有力地指导智慧园区企业构建起稳固可靠的网络安全防御体系，帮助企业有效应对日益复杂的网络安全挑战，增强园区整体网络安全防护能力，为智慧园区的稳定运行、数据安全以及企业的持续创新发展筑牢坚实的“网络安全城墙”，推动智慧园区在安全的网络环境中实现数字化转型与高质量发展，也为整个智慧园区行业的网络安全标准化建设提供了关键的参考依据，引领行业网络安全保障水平迈向新台阶。

《网络安全人才实战化训练环境建设规范》正式发布

近日，由奇安信科技集团股份有限公司、湖北经济学院、武汉市网络安全协会、湖北省教育装备行业协会等多家单位共同起草的《网络安全人才实战化训练环境建设规范》在全国团体标准信息平台正式发布。这一标准的出台，为网络安全人才培养提供了全新的指南与规范，将有力促进网络安全人才培养体系的完善与发展，提升网络安全人才的专业素养与实战能力。

随着数字化时代的加速发展，网络安全已成为国家安全与社会稳定的重要基石。然而，当前网络安全领域面临着严峻的人才短缺挑战，对具备实战能力的专业人才需求极为迫切。在此背景下，众多业内知名企业、高校及行业协会携手合作，精心制定了《网络安全人才实战化训练环境建设规范》。

该标准涵盖了网络安全人才培养的多个关键维度，包括网络安全体系规划能力、信息系统安全防护保障能力、数据库安全与管理能力、数据备份与恢复能力、网络协议分析能力、网络安全技术应用能力、网络安全设备部署配置、移动网络与云安全技术、攻防实战、应急响应及运维综合能力等。通过建立全面且系统的网络安全实战化人才培养体系，致力于培养出既拥有扎实专业基础知识，又具备强大实战化网络安全能力的高素质人才。

该标准的发布，将对网络安全人才培养的各个环节产生深远影响。在教育教学方面，为高校及职业院校的网络安全专业课程设置、教学资源建设、实践教学环节设计等提供了明确的参考依据，有助于提升网络安全人才培养的质量与效率。在企业人才培训方面，为企业制定网络安全人才培训计划、搭建实战化训练平台提供了标准化的指导框架，助力企业快速培养出符合自身需求的实战型网络安全人才。在行业整体发展层面，将进一步推动网络安全行业的规范化与标准化进程，促进网络安全产业的健康、可持续发展。


团 体 标 准

网络安全人才实战化训练环境建设规范

Standard for the Construction of Practical Training Environment for Network Security Talents

2024-11-26 发布 2025-1-1 实施

武汉市网络安全协会 发布

未来，各起草单位将继续携手合作，积极推动《网络安全人才实战化训练环境建设规范》的落地实施，通过开展培训、研讨会等多种形式的活动，加强标准的宣传与推广，确保更多的网络安全人才培养机构、企业及从业者能够深入理解并应用该标准。同时，各方也将持续关注网络安全行业的发展动态与技术创新，适时对标准进行修订与完善，为网络安全事业的发展提供源源不断的人才支撑与智力保障。

《制造业数据安全管理中的数据分类分级方法指南》正式发布

近日，由武汉市网络安全协会、智网安云（武汉）信息技术有限公司、华中师范大学、湖北大学等多家单位共同起草的《制造业数据安全管理中的数据分类分级方法指南》于全国团体标准信息平台正式发布。

在数字化浪潮汹涌的当下，制造业正加速数字化转型，数据量呈爆发式增长，数据安全管理已成为制造业发展的重中之重。其中，数据分类分级更是筑牢数据安全防线的核心环节。

此指南聚焦制造业企业需求，精心构建了一套科学且实用的数据分类分级方法体系。其明确了数据分类分级的基本原则、严谨流程以及具体操作方法。这将成为制造业企业管理和保护数据资产的得力助手，助力企业显著提升数据安全管理效能，有效降低数据安全风险，保障制造业数据的安全性、可靠性，并促进数据的高效利用。

该指南不仅为制造业企业的数据安全实践提供了关键指引，还将为相关行业标准的进一步制定与完善贡献宝贵经验与智慧源泉，有力推动制造业数据安全管理朝着规范化与标准化的方向稳步迈进，为整个制造业的数字化健康发展奠定坚实的基础，在数据安全的保驾护航下，助力制造业在数字经济时代乘风破浪，稳健前行。

在汉高校网络安全应用场景供需对接会圆满落幕 校企携手共筑新防线 供需对接共创新纪元

为深入学习贯彻习近平总书记关于网络强国的重要思想和关于网信工作的重要指示精神，进一步深化在汉高校与网络安全产业之间的合作，推动网络安全技术与各领域应用场景的深度融合，常态化机制化推动网络安全应用场景对接，6 月 25 日，在省委网信办、省教育厅的支持下，在武汉市委网信办、东西湖区人民政府的指导下，临空港经开区现代服务产业建设管理办公室会同武汉市网络安全协会在国家网络安全人才与创新基地网安创新中心成功举办了“在汉高校网络安全应用场景供需对接会”。

此次对接会，旨在搭建一个高校与企业深入交流、供需精准对接的平台，共同探索网络安全产学研用创新发展之路。活动吸引了在汉六十余所高校网信工作负责人及部分计算机与网络安全院系负责人，同时汇集了四十家网络安全领域的领军企业参与。

国家网络安全人才与创新基地作为武汉市推动科技创新和高质量发展的新引擎，多年来在中央网信办和省市相关部门的有力指导下，不断夯实基础、提升能力，着力打造成为网络安全领域的人才高地、创新高地和产业高地。此次对接会的成功举办，正是网安基地联手行业协会共同推动高校与企业紧密合作、共谋“产学研用”协同发展的重要举措。

对接会上，各方代表们就网络安全领域的最新技术趋势、应用场景需求、人才培养等方面进行了深入交流和探讨。高校负责人纷纷表示，通过此次对接会，更加直观地了解到了企业的实际需求和技术趋势，也认识到了高校在网络安全领域可以发挥的重要作用。他们期待与基地及更多企业展开深度合作，共同推动网

对接会现场

络安全技术的创新和发展。

活动现场很多高校和企业代表纷纷向活动主办方表示：

武汉大学网络安全与信息化领导小组办公室副主任蔡利军：

“这次对接会是一个难得的机遇，让我们有机会深入了解网络安全领域的最新技术和市场需求。作为高校网络安全工作的负责人，我们深知责任重大。我们将与相关基地、协会以及企业展开密切合作，加强网络安全领域的人才培养与科研创新工作，致力于为网络安全领域输送更多高素质的专业人才，共同筑牢我校在网络安全方面的坚实防线。”

武汉轻工大学数学与计算机学院软件工程系系主任张帆：

“作为‘政产学研用’的重要一环，对接会不仅提供了政府机构、企业、高等院校、科研机构和实践运用五个主体之间强化联系的平台，而且促进了技术创新上、中、下游与最终用户的对接和耦合。在对接会上，我们欣喜地看到了国产网络安全技术和产品的高速发展，但同时也对于高质量地培养网络安全人才以满足国家、地方、企业和社会的需求深感责任重大。作为省属普通高校的一员，我们将力求找准自身定位，努力培养具有丰富工程实践经验和优秀工程创新能力的网络安全本科和硕士人才，服务于国家战略，服务于我省、我市的发展规划。”

武汉交通职业学院现代教育信息中心主任沈卫文：

“这次对接会为我们搭建了网络安全保障工作与行业前沿技术的对接桥梁。作为高校网信工作负责人我们深感责任重大，我们将与专业学院、基地、协会和企业紧密合作，推动学校网络安全保障工作与网络安全领域人才培养的融合，践行多元协同育人。在筑牢我校网络安全屏障的同时，为网络安全领域输送更多高素质的专业人才。”

武汉市网络安全协会民办高校工作委员会主任俞全：

“此次对接会一方面提供了一个了解学习网安领域最新资讯和技术的平台，更重要的是引发我们民办高校

对下一步如何继续做好高校网络安全工作的思考。网络安全在高校数字化转型中充当着坚实的后盾，关系到学校的正常运营，需要汇聚多层力量共同守护。作为民办高校网络安全守护者的一份子，我们将持续与基地、协会和相关企业保持密切沟通合作，共同努力，为网络安全事业贡献自己的一份力量。”

武汉商贸职业学院现代信息技术学院常务副院长骆泓玮：

“加强网络安全建设，培养网络安全技术人才，以确保网络空间的安全稳定，从而为国家的整体安全提供坚实保障。我校非常重视校园网络安全工作，此次安排了我校信息学院、智能中心的教师和技术人员参加今天活动，收获很大。现场多家网络安全企业参展，展示了最新技术。这次会议对加强校企合作，产教融合，共同提升网络安全具有重要意义。”

武汉金银湖实验室众测竞测平台部项目经理刘飞雪：

“在这次对接会上，我们深切感受到与高校合作在网络安全领域的重要性，不仅能满足学校对安全建设的需求，也能为实验室引入急需的网络安全人才。我们期待与各高校深化合作，共同提升网络安全水平，培养更多专业人才，携手为构建更安全的网络环境作出贡献。”

360 数字安全集团湖北办事处负责人李婷：

“通过参加本次高校供需对接活动，让公司在与高校的业务合作和发展上有了更清晰的方向。未来在网







络安全领域融合人工智能技术发展，共同孕育实战型人才培养，以及前沿科技领域的科研合作等诸多方面带来蓬勃发展空间。”

湖北天融信网络安全技术有限公司政府事业部总经理吕露：

“没有网络安全就没有国家安全，网络空间安全是国家安全的重要组成部分。网络空间竞争，归根结底是人才竞争。天融信秉承“融天下英才 筑可信网络”的理念，是最早开展网络安全培训的安全企业，我们深知高校是人才培养和聚集的主要阵地，也是国家战略科技力量的主要组成部分。我们希望通过此次大会，共同推进校企联合培养中心，推动网络安全教育、技术、产业融合发展。持续深化产教融合，致力于打造具有中国特色的网安人才培养新生态。”

武汉吧哒科技股份有限公司教育行业黄旸：

“近年来，随着信息等级保护建设，各高校安全能力已初具模型。但许多高校依然面临着安全管理制度不完善、资产管理困难以及安全工作无闭环等管理问题。为此，我司基于多年的安全服务能力及研发能力，自研了多款款非常适合高校场景的安全管理创新产品。我们感谢活动主办方为我们提供与各高校交流互动的机会，希望我们有机会能为各高校网络安全管理工作，提档加速。”

湖北天地和兴科技有限公司副总经理汪立志：

“今天的在汉高校网络安全应用场景供需对接会活动，不仅为湖北天地和兴科技有限公司提供了网络安全领域的专业实力的展示机会，也为高校与企业之间搭建了一个交流与合作的桥梁，推动了网络安全行业的产教融合与技术创新。这场活动无疑为武汉市乃至整个湖北省的网络安全产业发展注入了新的活力，也为未来网络安全领域的发展指明了方向。”

武汉艾迪时代网络技术有限公司总经理向杰：

网络安全在汉高校对接会为高校和企业搭建了一个交流与合作的平台，通过人才培养、课程共建、科研项目合作、实验室共建、产学研基地等产教融合的合作模式，有助于共同培养更多优秀的网络安全人才，推动网络安全产业的发展。

武汉粟泰信息科技有限公司总经理许鹏：

“没有网络安全，就没有国家安全”网络安全和信息化对一个国家很多领域都是牵一发而动全身的，而教育领域更是一个国家的根本，是祖国的未来；我们的数据中心基础设施全网能解决方案已应用于湖北各高校，为其信息安全保驾护航。这次对接会给我们提供了更多宝贵的资源和合作机会。接下来我们将进一步加强与高校的合作，共同推进网络安全人才与技术的蓬勃发展，助推网络安全产业的的蓄力腾飞。

任子行网络技术股份有限公司湖北经理龙勇：

“通过与高校的合作，任子行网络技术股份有限公司整合各方面的资源和技术力量，共同攻克网络安全难题，提高网络安全防护的整体水平。同时促进高校产学研用各方的深度融合，加速网络安全技术的创新和成果转化，推动产业的发展。”

同时，网络安全企业代表热切期盼高校能开放更多应用场景，与各高校在优化校园网络环境、强化网络运维服务、保障网络绿色安全稳定等方面携手共进。同时，他们也希望能充分发挥高校的科研和人才资源优势，通过资源共享优势互补，共同推动网络安全技术的创新与进步，引领网络安全产业迈向新的高度，为构建网络强国贡献力量。

在对接会现场，各企业的展台设计新颖、内容丰富，充分展示了最新的网络安全技术、产品和解决方案。现场还举办了多场技术交流和对接活动，为高校与企业之间搭建了直观、高效的沟通平台。通过深入探讨和交流，代表们纷纷表示，此次对接会不仅为他们提供了宝贵的学习和交流机会，也为未来在网络安全领域的合作奠定了坚实的基础。

展望未来，武汉市网络安全协会将继续发挥协会桥梁纽带作用，联合各方力量，支撑好国家网络安全人才与创新基地建设，加大我市各领域网络安全的宣传和投入，推动高校与企业之间的紧密合作，常态化开展各领域应用场景对接，共同打造网络安全交流合作平台，为筑牢国家网络安全屏障贡献武汉力量。

人保财险武汉市分公司加入武网安协 助力武汉数字经济安全发展

近日，中国人民财产保险股份有限公司武汉市分公司（以下简称：人保财险武汉市分公司）正式成为武汉市网络安全协会会员单位。7 月 3 日，武汉市网络安全协会党支部书记、秘书长刘悦恒、网络安全保险工作委员会秘书长周韬及公共关系发展部主任严媛等协会相关负责人一行，走访了人保财险武汉市分公司，并举行了授牌仪式。

人保财险武汉市分公司党委委员、总经理助理苏彦红对协会一行的到来表示了热烈的欢迎，介绍了公司的基本情况、发展历程以及在科技保险领域的积极探索。他强调：“在数字经济发展的推动下，网络安全已成为国家安全的重要组成部分。面对日益复杂的网络环境，人保财险作为中国内地最大的财产保险公司，历史悠久、业务规模大、综合实力强，深感责任重大，人保将继续发挥保险优势，为客户提供更加全面、专业的网络安全保险产品及服务，促进各行各业加强网络安全风险管理，共同推动网络安全产业高质量发展，助力制造强国、网络强国建设。”

座谈会上，人保财险武汉市分公司东西湖支公司总经理何边围绕当前网络安全形势、国家政策导向以

及人保财险在网络安全保险领域的创新实践进行了深入剖析。他表示，公司将积极响应国家号召，借助国家网络安全人才与创新基地优势资源，不断优化产品设计，提升服务水平，以更好地满足市场需求。

武汉市网络安全协会党支部书记、秘书长刘悦恒热烈欢迎人保财险武汉市分公司的加入协会，并详细介绍了协会在推动网络安全生态建设方面的努力与成果。他强调：“网络安全保险是为网络安全风险提供保险保障的新兴险种，日益成为转移、防范网络安全风险的重要工具，在推进网络安全社会化服务体系建设中发挥着重要作用。近年来国家高度关注网络安全保险的发展，出台了相关指导意见，武汉网安协会率先在华中成立了网络安全保险工作委员会。我们期待与人保财险携手并进，共同探索网络安全 + 保险 + 服务的新模式，为提升我市网络安全防护能力、促进数字经济健康发展贡献力量。”

网络安全保险工作委员会秘书长周韬详细阐述了网络安全保险的发展现状、未来趋势以及协会在此领域的工作规划。他指出，随着网络安全事件的频发，企业对网络安全保险的需求日益迫切。协会将充分发挥桥梁纽带作用，通过不断的标准供给和平台建设，打通网安与保险之间行业沟通屏障，帮助保险企业快速识别评价投保单位安全风险和网络安全服务质量，推动保险行业与网络安全产业的深度融合，为企业提供更加精准、高效的网络安全风险解决方案。

座谈交流环节，与会人员围绕网络安全保险的发展趋势、风险评估、产品设计、理赔服务等议题展开了深入讨论。大家一致认为，面对数字化转型的浪潮，加强网络安全保险的合作与探索具有重要意义。双方将以此次合作为契机，进一步整合资源、创新模式、优化服务，共同推动武汉网络安全 + 保险事业迈向新的高度。

网络安全无小事，常态抓实筑防线
经开区2024年教育系统网络安全培训成功举办

7月4日，由武汉经开区教育局主办、市网络安全协会协办的经开区教育系统网络安全培训活动成功举办，全区各公、民办中小学、幼儿园以及局机关科室的相关人员参加了此次培训活动。培训持续一天，为全区教育工作者带来了一场网络安全知识的盛宴。

活动开场，经开区教育局信息办黄磊主任强调："网络安全是教育系统的重中之重，直接关系到每一位师生的切身利益与校园的稳定发展。面对信息技术的飞速发展，网络安全威胁日益严峻，我们每一位教育工作者都应当站在维护国家安全和社会稳定的高度，充分认识网络安全工作的重要性。"

江汉大学人工智能学院（研究院）副院长、精细爆破国家重点实验室爆破数字化研究所所长、硕士生导师、市网络安全协会专家邓宏涛教授，以其深厚的学术造诣和丰富的实践经验，为参训人员深入解读了当前网络安全政策与网络安全工作的重点。邓教授不仅阐述了国家层面对于网络安全的重视与部署，还结合教育系统的实际情况，提出了切实可行的防护策略与建议。

随后，武汉市网络安全协会党支部书记、秘书长刘悦恒，就网络安全产业的最新动态与技术趋势进行了深入浅出的讲解。刘秘书长通过生动的案例和详实的数据，展示了网络安全技术的飞速发展及其在保护国家安全、社会稳定和个人隐私方面的重要作用，激发了参训老师对网络安全事业的浓厚兴趣与热情。

江汉大学人工智能与大数据实验中心主任、市网络安全协会专家叶锋副教授，围绕网络数据安全治理体系进行了详细的阐述。叶副教授从数据安全的基本概念、治理原则、管理体系构建等方面入手，为参训人员描绘了一幅清晰的数据安全治理蓝图。他指出，数据安全治理需要全校上下共同参与，形成合力，才能确保数据的安全与可控。

江汉大学人工智能学院科研秘书、精细爆破国家重点实验室爆破数字化研究所副所长、陈子琪副教授，从网络数据安全风险与防护的角度出发，通过生动的案例分析，揭示了网络数据安全面临的种种威胁与挑战，并介绍了多种实用的防护技术与策略。他的演讲既具有理论深度，又贴近实战需求，让老师们受益匪浅。

通过一天的紧张学习与交流，参训人员不仅掌握了最新的网络安全知识与技能，还深刻认识到了网络安全工作的重要性与紧迫性。大家纷纷表示将把所学知识与实际工作相结合，积极推动网络安全工作的深入开展，为经开区教育系统的稳定发展贡献自己的力量。

黄主任在活动总结时向大家提出了四点殷切期望：一是所有单位必须高度重视网络安全工作，任何疏忽都可能带来不可估量的后果；二是各学校要迅速行动，落实网络安全专项负责人制度，明确职责，确保工作有人抓、有人管；三是要加强网络安全教育，将网络安全知识纳入日常教学内容，提升师生及家长的网络安全意识与防范能力；四是各单位要切实加强对电子设备、网站平台等关键环节的专项管理，建立健全信息安全管理制度，确保信息安全无虞。

此次培训活动的成功举办，不仅提升了全区教育工作者的网络安全意识与防护能力，更为构建安全、和谐、稳定的教育网络环境做出了积极探索。

武汉市网络安全协会民办高校工作委员会2024年第一次工作会议成功举办 民办高校共议网安 东湖倡议共筑屏障

2024年7月6日，武汉市网络安全协会民办高校工作委员会二〇二四年第一次工作会议在武汉东湖学院嘉鱼校区隆重召开。此次会议汇聚了近二十所民办高校的领导、网信部门负责人、专家学者及相关行业精英，共同研讨民办高校网络安全与信息化建设的工作经验和发展路径。会议由协会民办高校工委会主任、武汉设计工程学院信息中心主任俞全同志主持。

武汉东湖学院董事、党委常委、副校长胡榆同志对与会嘉宾的到来表示热烈的欢迎。他指出，高校作为知识传承和人才培养的摇篮，必须积极应对网络安全挑战，为培养高素质人才创造安全的育人环境。同时，他对本次会议和工委会的工作寄予厚望，期待通过深入交流与合作，共同推动民办高校领域的网络安全和信息化工作取得新突破。

武汉市网络安全协会秘书长刘悦恒同志对东湖学院热情周到的安排表示感谢。他表示，武网安协将依托和支持工委会作为平台，不断促进网络安全产业与民办高校间的交流与合作，不断强化安全责任担当，鼓励网安技术创新，打通产学研用各方链条，筑牢校园网络安全屏障。

会上，武汉东湖学院信息中心主任田斌同志作了报告分享，详细介绍了学校在网络安全体系建设、人才培养、技术创新等方面的实践经验与成果。他通过具体案例分析，展示了学校在应对网络攻击、数据保护、信息系统安全等方面所采取的有效措施，为其他高校提供了有益的参考和借鉴。

随后，武汉学院信息中心主任肖磊同志进行了信息化工作分享，全面展示了学校在信息化建设方面的规划、实施和成果，包括智慧校园平台的搭建、信息化教学手段的应用、数据治理与共享等方面的创新举措。他还分享了推进网络安全和信息化工作过程中遇到的困难和解决办法，为其他高校提供了宝贵的经验和启示。

武汉信息传播学院陈明怀同志带来了金融支付中台案例分享，详细剖析了金融支付中台在校园场景中的应用，包括如何保障支付安全、优化支付流程、实现资金的高效管理等。这一案例展示了金融科技在高校领域的创新应用，为提升校园服务水平和管理效率提供了新的思路。

在下午的会议研讨环节，各民办高校代表踊跃发言，就网络安全工作领域的经验与挑战进行了深入交

流。与会代表围绕网络安全人才培养机制、技术创新路径以及教育信息化水平提升等核心议题展开了富有成效的讨论。

武昌理工学院信息中心主任郭红艳同志表示，网络安全工作需从多方面采取措施，学校应从管理措施和技术手段两方面着手，确保师生网络安全。同时，她建议上级主管部门在网络安全检查工作中优化程序，更多地关注和帮助学校做好安全防护工作。

民办高校特聘专家江诗敏同志指出，民办高校在网络安全方面普遍存在安全意识薄弱、技术滞后、管理不完善等问题。他呼吁在协会及工委会的倡导下，各高校提高认识、持续加大投入，加强网络安全教育、更新网络安全技术、建立网络安全管理体系，并加强对外合作与交流。

武汉城市学院信息中心主任易锵懿同志建议，建立信息化和网络安全工作的同步机制，实现制度化和流程化处理，使网络安全和信息化成为推动学校发展的双翼和双轮，在解决网络安全问题的同时解决数据共享问题。

武汉学院信息中心主任肖磊同志认为，民办高校因具有一定特殊性，工委会可不断结合国家法规和主管部门要求，总结各民办学校共性问题，编制更适合民办高校办学情况的网络安全工作标准和指导性文件，不仅能提升学校管理水平，增强师生防护意识和能力、保障教育网络数据安全，还能提升学校形象和声誉，促进教育数字化健康转型。

会议最后，代表们针对民办高校网络安全工作的特点并结合本次会议中大家的共识，形成了《民办高校网络安全工作倡议书—东湖倡议》，经工委会全体审议，全票予以通过。

工委会主任俞全同志表示，《东湖倡议》的通过，体现了民办高校工委会在网络安全工作中的责任与担当，倡议从网络安全意识到制度、技术到应急响应、共治与文明上网等多方面工作进行了约定，对民办高校网络安全工作有很强的参考和指导价值。网络安全关乎每个人的切身利益，更关乎社会稳定和国家安全，热情期待全省全国更多高校的积极响应和加入，工委会愿与各高校携手同行，共同守护好这片校园网络净土。

会后，与会代表还实地参观了东湖学院智慧教室、网络机房和图书馆等学校建设情况，直观感受了东湖学院新一代智慧校园建设的成果和网络安全工作取得的突出成效，大家纷纷表示将探索相关成果在本校的应用。

本次会议的成功举办为武汉民办高校的网络安全与信息化建设搭建了学习互鉴、交流合作的平台，明确了未来的发展方向和重点任务。相信未来，在各方的共同努力下，民办高校的网络安全与信息化水平将不断提升，为高等教育事业健康发展提供更为坚实的支撑保障。

《东湖倡议》
——民办高校网络安全工作倡议书

为深入学习习近平总书记关于网络强国的重要思想，贯彻《网络安全法》《数据安全法》《个人信息保护法》《党委（党组）网络安全工作责任制实施办法》等法律法规，积极响应国家教育数字化战略，营造安全、健康、和谐的校园网络环境，依托武汉国家网络安全人才与创新基地资源优势，武汉市网络安全协会民办高校工作委员会，在武汉东湖学院召开的 2024 年第一次工作会议上，向工委会成员及同类兄弟院校发出以下倡议：

一、提高网络安全意识，强化宣传教育

加强宣传教育：各民办高校应积极开展网络安全宣传教育活动，通过讲座、研讨会、在线课程等形式，普及网络安全知识，提高师生的网络安全意识和防护能力。制定不同群体的培训计划，确保宣传教育效果。

培养良好习惯：引导师生树立正确的网络使用观念，养成安全上网、文明上网的良好习惯，不随意点击不明链接，不下载不明软件，不泄露个人信息，共同维护网络空间的安全与秩序。

二、完善网络安全制度，托起安全责任

建立健全网络安全管理制度：各民办高校应制定和完善网络安全管理制度，明确网络安全管理职责和流程，确保网络安全工作有章可循、有据可查。结合《党委（党组）网络安全工作责任制实施办法》，制定本校的实施细则，明确各级责任体系。

加强网络安全监测与预警：建立网络安全监测体系，对校园网络进行实时监控和预警，及时发现并处置网络安全事件，保障校园网络的安全稳定运行。同时，常态化开展网络安全检查和考核，确保各项制度得到有效执行。

三、加大网络安全投入，筑牢安全防线

加大网络安全技术投入：定期升级校园网络环境中的软硬件设备，及时升级和更新病毒库、漏洞库等，确保网络安全设备的技术先进性和持续防护能力。构建高效数字化协同指挥机制，整合学校各部门资源，形成协同防护能力。

加强数据加密与备份：对重要数据和敏感信息进行加密处理，并定期进行数据备份和恢复演练，确保数据的安全性和完整性。利用大数据技术建立可信赖的数字化安全数据中台，实现安全数据的集中存储、分析和应用，提升安全响应效率。

四、定期演练及时响应，提升应对能力

制定应急预案：各民办高校应制定网络安全应急预案，明确应急响应流程和处置措施，确保在发生网络安全事件时能够迅速、有效地进行处置。

组织应急演练：定期开展网络安全应急演练活动，提高师生应对网络安全事件的能力和水平。通过模拟攻击、钓鱼测试等手段，检验应急预案的有效性，不断优化和完善应急响应机制。

五、构建合作共治格局，形成工作合力

加强校企合作：与网络安全行业组织、企业、公立高校之间建立紧密的合作关系，形成“产学研用”的科研转化 + 产教融合协同育人的新模式新机制，不断提升学校网络安全科研与人才队伍水平。积极借助国家网络安全人才与创新基地优势，参加国内、国际网络空间安全学术交流合作，发出武汉民办高校的声音和主张。

推动社会共治：积极与党政国家机关、企事业单位、社会团体等单位合作，共同打击网络犯罪行为，营造清朗的网络空间。加强与公安、网信等部门的沟通协调，畅通情报信息，形成工作合力。

六、提升素养文明上网，清朗网络空间

传播正能量：鼓励师生在网络上传播正能量信息，弘扬社会主义核心价值观和中华民族优秀传统文化。利用校园网络平台和社交媒体，宣传网络安全知识和文明上网理念。

抵制网络谣言：教育师生不信谣、不传谣、不造谣，共同维护网络空间的清朗和秩序。及时发现并处置网络谣言，防止谣言扩散造成不良影响。

网络安全工作是一项长期而艰巨的任务。我们呼吁各民办高校积极响应本倡议，共同努力、携手并进，以高度的责任感和使命感，为营造安全、健康、和谐的校园网络环境贡献自己的力量！

武汉市网络安全协会民办高校工作委员会

2024年7月

中国新闻网报道武网安协工作成果

原标题：布局新兴产业武汉实现的那些行业“第一”

近日，在中国网络社会组织联合会与中国新闻网联合开设的“共筑网上网下同心圆，社会组织在行动”的专栏中，经评审推荐，我会相关工作成果得到关注和宣推。

党的十八大以来，在习近平新时代中国特色社会主义思想特别是习近平总书记关于网络强国的重要思想指引下，中国网络社会组织联合会积极发挥桥梁纽带作用，积极倡导行业自律，引导行业企业健康发展，传播网络正能量，取得积极进展。为进一步提高政治站位，团结凝聚网络社会组织，为推进网络强国建设贡献力量，特会同中国新闻网等会员单位，共同开设“共筑网上网下同心圆：社会组织在行动”专栏，梳理展示网络社会组织助力网信事业发展的积极探索和生动实践，与读者交流分享。

我会作为中国网络社会组织联合会正式成员与武汉网络安全产业的代表，多年来坚持带领成员单位积极主动对接国家级平台资源；并与各地兄弟省市网络安全协会广泛开展交流合作；参与了省市网络安全领域各类的课题研究、政策咨询与制定工作；参与并组织历年省市“国家网络安全宣传周”系列宣传活动；主办承办了各类型专业性论坛、赛事、全市攻防演练等大型活动；协助主管部门开展重要专项等工作，为全市网络安全工作做出了积极贡献。

光明网发表我会署名文章：加快推进网络安全创新发展

近日，光明网发表了我会专家曹越教授、秘书长刘悦恒署名文章：加快推进网络安全创新发展。

原文如下：

习近平总书记多次强调“没有网络安全就没有国家安全”，凸显了我国网络安全保障的重要性。面对新形势下网络安全的新挑战，仍需深入研究与全面理解网络空间治理的重要性，以期更好提升网络安全防范及应对能力，捍卫国家安全与人民利益。

我国网络安全工作取得积极进展图片

近年来，我国网络安全顶层设计、机制体制与工作体系不断完善，安全防护保障能力持续增强，全民网络安全意识和技能不断加强，网络安全方面的关键性前沿技术更是不断突破，并取得了显著成就，已为我国网络安全建设提供了坚实的技术支撑与强大保障，提升了网络空间综合治理水平。

一是顶层设计和全面布局持续加强。党中央对网信工作的集中统一领导持续加强，中央、省、市三级网信工作体系基本建立，县级网信机构建设扎实推进。强化网络安全与信息化领域顶层设计、总体布局、统筹协调、整体推进及督促落实，并统筹推进网络安全领域重要任务、重大项目、重点工程。

二是网络安全政策体系不断完善。我国于多个领域及层面已进行了全面战略布局与规划，以总体国家安全观为引领，推出了《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等网络安全领域的基础性、框架性、综合性法律法规。同时，通过实施《关键信息基础设施安全保护条例》《网络安全审查办法》《云计算服务安全评估办法》等具体规定，构建了坚实的网络空间数据安全保障基础。特别是近年来，针对智能网联汽车、工业控制等新兴产业领域，我国及时出台了《车联网网络安全和数据安全标准体系建设指南》《工业控制系统网络安全防护指南》等专项法规，以推动特色产业安全保障体系的快速建设，确保新兴产业也能够健康、稳定、可持续地发展。

三是推动网络安全产业生态完善与技术创新。目前，人工智能、机器学习等前沿技术已广泛融入网络安全领域，显著提升了安全防护效率及准确性；同时，区块链技术的运用确保了数据于交互过程中的安全性与防篡改性，特别契合数字经济时代对数据要素保护的高要求。此外，国产密码技术在关键信息系统中更加广泛地应用，也为网络安全提供了坚实的保障。与此同时，为了进一步加强密码技术的研发和应用，国家已设立了密码科学与技术专业一级学科，致力于培养高层次密码应用型人才；而零信任网络安全框架的提出，强调了对网络内外实体的严格控制及身份验证，为各行业提供了更为严密及可靠的网络安全保护；在卫星网络安全领域，我国同样注重技术创新及应用，以确保卫星通信的安全及稳定。上述技术的发展和应用，共同推动了我国网络安全产业向更高水平迈进。

四是共筑网络安全防线，网络生态持续向好。网络空间主流思想更加鲜明，正能量更加充沛。我国已连续举办九届全民国家安全教育日、十届国家网络安全宣传周主题活动，致力于提高全社会对网络安全的认识，加强网络安全教育与培训，推广网络安全知识与技能，营造健康文明的网络环境；同时，网络综合治理体系不断完善，网络基础设施建设步伐不断加快，出台了《关于加快建立网络综合治理体系的意见》，为经济社会发展提供了有力支撑。

面向未来重点布局规划 共筑网络安全坚强防线

西方发达国家已于网络信息安全技术、网络空间治理规则及网络空间安全人才储备等方面进行了深入且周密的战略布局，网络空间已成为全球战略竞争的新领域，其安全战略博弈与攻防问题对于维护国家安

全和提升国际竞争力具有重要意义。其中，关键信息基础设施是网络安全的重中之重；人才是网络安全建设的核心驱动力；数据安全是网络安全的基础，数据安全风险日益成为影响产业发展、网络安全甚至国家安全的重要因素。针对当下复杂的网络安全形势，我国作为网络空间领域的后来居上者，要从上述三个方面进行重点布局与规划。

一是积极应对关键信息基础设施面临的风险挑战与机遇。关键信息基础设施是网络安全的重中之重，是关乎国家安全的命门所在。随着智慧城市的蓬勃建设，我国于新基建领域取得了显著成就，然而日益复杂的网络安全威胁给新基建发展造成了巨大挑战。一方面，我国在 2021 年就已部署共 16 座“双智”试点城市，在智慧城市运维中所面临的网络安全风险，不再仅仅是信息泄露、信息系统无法使用等问题，而是会对现实世界造成直接、实质性影响，如交通瘫痪、城市运行停滞等运维风险，其中针对关键信息基础设施的网络攻击已演变成为全球性问题，尽管我国关键信息基础设施发展迅速，但同时也是全球遭受网络安全威胁最严重的国家之一。为此，针对关键信息基础设施运维过程中面临的多样化、复杂化网络攻击与威胁、技术漏洞与风险隐患等，需大力加强人工智能、区块链、量子计算等前沿技术的开发与应用，以构筑关键信息基础设施网络空间的信任生态体系。另一方面，变动的世界迫使我国重新审视关键信息基础设施安全发展中的重要性与不足之处，除加强网络安全防护方面，战争或将破坏基础设施建设，这不仅要求关键信息基础设施采取物理安全措施，确保设施免受破坏，更强调了重视网络空间的安全性及可靠性，建立容灾备份与应急服务措施。

二是长远布局网络空间安全人才的培养与体系建设。据《网络安全人才实战能力白皮书》数据显示，截至 2027 年，我国网络安全领域的人才缺口预计将高达 327 万人，高校每年仅约 3 万名专业毕业生的巨大供需差距，仍凸显了网络安全人才培养的紧迫性。此外，网络安全人才不仅需具备扎实理论知识，更需具备实战能力。更为严峻的是，网络安全人才与行业的融合度尚显不足，特别是于车联网安全、卫星互联网安全、社会治理等行业关键领域的复合交叉型专业人才匮乏。在此形势下，迫切需要培养一支高素质创新型复合型实战型应用型的网络安全人才队伍，建议加强产学研用深度融合，建立匹配特色产业需求的网络空间安全人才评价体系，加强包含网络安全意识、关键技术、知识理论及创新实践等维度在内的培养体系建设，形成多层次多元化的复合型人才培养模式。

三是维护数据网络安全，夯实网络强国安全“基座”。随着全球化进程不断加深与数字技术的快速发展，数字经济已经成为全球经济增长的新引擎。而数据作为新型生产要素，已成为社会数字化、网络化与智能化发展进程的基石，逐渐融入社会生产、分配、流通、消费及服务管理等各个环节，对生产方式、生活方式及社会治理方式产生深刻影响。然而，数据要素的发展面临数据隐私及安全风险问题，随着数据大规模增长与数据要素处理，个人敏感信息及机密业务数据面临持续扩大性风险，包括数据要素的泄露风险、滥用风险、篡改风险及规范问题。此外，数据收集、整合及处理过程中确保数据质量与可信度也是另一重要问题，而数据权属、法律伦理等方面也需要持续密切关注。为此，需加强加密技术、身份认证技术、访问控制等技术手段，提高数据安全性及保密性，同时开展数据安全风险评估及监测预警，及时发现并应对数据安全风险，共建数据网络安全环境，为数字经济的健康发展提供有力保障。

面向新时代新征程，我国需要坚持以习近平总书记关于网络强国的重要思想为指导，不断深化网络安全领域的创新与发展，积极应对新征程上网络安全面临的风险挑战与机遇，为推进网络安全与信息化协同发展、早日实现网络强国作出更大贡献。

我会助力全国首单电力行业政策性网络安全综合保险落地武汉光谷

8月1日，全国首单电力行业政策性网络安全综合保险在武汉市东湖高新区（光谷）成功落地。该保险由武汉市网络安全协会会员单位——中国人民财产保险股份有限公司武汉市分公司签发，标志着武汉光谷在全国电力行业在网络安全保障方面迈出了重要一步。通过创新的“保险＋服务＋科技”模式，该保险为东湖高新区现代服务园内的武汉映瑞电力科技有限公司提供了全面的网络安全风险保障。

电力行业作为国家关键信息基础设施的核心领域，正加速向信息化、数字化、智能化转型，电力企业在网络安全领域的风险保障需求日益凸显。为了满足这一需求，武汉市网络安全协会网络安全保险工作委员会与武汉东湖科技保险发展促进中心联合保险机构，借助工委会核心成员单位武汉华康科技有限公司的数字安全风险快速量化评级平台，实现了保险产品与网络安全专业服务的深度融合。该平台为网络安全风险缓解和转移提供了全流程线上一站式闭环服务，涵盖企业投保前的风险量化评估、保中持续风险监测追踪、风险跟踪处置、特定风险的转移、随时随地一键全生态风险报告等保前保中与保后过程，助力企业在数字经济时代提升数字化资产安全防护水平和风险对抗能力，为企业持续提供网络安全风险量化管理服务和风险保障。

本次网络安保险的成功落地，不仅为武汉映瑞电力科技有限公司等企业提供了有力的网络安全保障，也是各方为积极落实工业和信息化部与国家金融监督管理总局联合发布的《关于促进网络安全保险规范健康发展的意见》作出了有益探索。该意见指出：网络安全保险是为网络安全风险提供保险保障的新兴险种，日益成为转移、防范网络安全风险的重要工具，在推

进网络安全社会化服务体系建设中发挥着重要作用。该意见还特别强调：鼓励重点行业企业完善网络安全风险管理机制，推动电信和互联网、制造业、能源、金融、交通、水利、教育等重点行业企业积极利用网络安全保险工具，有效转移、防范网络安全风险，提升网络基础设施、重要信息系统和数据的安全防护能力。支持中小企业通过网络安全保险服务监控风险敞口，建立健全网络安全风险管理体系，不断加强中小企业网络安全防护能力。

武汉市作为拥有全国首个国家网络安全人才与创新基地以及唯一国家级科技保险示范区的城市，正积极开展网络安全保险服务试点工作。目前，武汉市网络安全协会网络安全保险工作委员会在各级主管部门的指导支持下，已联合成员单位开展多场政策性宣贯会、培训会和研讨沙龙，并提交多份工作报告和建议书，开展各项前瞻性标准制定工作。

今后，工委会将进一步推动湖北武汉网络安全产业和金融服务的融合创新，按照国家各项法规要求，引导网络安全保险健康有序发展，培育新业态，促进企业加强网络安全风险管理，为网络安全产业的高质量发展作出积极贡献。

我会召开网络安全定级专家评审会

近日，由武汉市网络安全协会组织的订单自动化受理平台及 OA 流程自动化平台网络安全等级保护定级评审会分别在协会召开，会议邀请了行业内专家对会员单位的订单自动化受理平台及 OA 流程自动化平台进行定级评审。

会上，首先由刘悦恒秘书长做项目评审工作介绍，围绕信息系统安全保护等级的划分与保护、定级工作的主要步骤进行介绍说明。

随后由平台运营使用单位对测评平台的项目背景、功能使用情况做简要介绍；依据国家标准《信息安全技术网络安全等级保护定级指南》GB/T 22240-2020，对定级报告进行评审。

最后，与会专家在听取定级测评平台的情况汇报后，审阅定级报告等相关材料，对平台从业务信息、数据存储、服务功能等多维度，经质询、讨论，形成报告整改建议，现场签署定级评审意见。

此次定级评审会的召开，为平台后续的网络安全建设和管理提供了重要的指导依据。同时，也为该企业不断提高平台的安全防护能力，保障平台的稳定运行奠定了坚实的基础。

武汉市网络安全协会获评 AAAA 社会组织称号

近日，根据武汉市民政局《2023 年度社会组织评估等级结果公告》，武汉市网络安全协会（以下简称“协会”）被评为 2023 年度“AAAA 级社会团体”。

根据民政部《社会组织评估管理办法》和《武汉市社会组织评估管理办法》规定及评估工作的有关要求，协会针对基础条件、内部治理、工作绩效、社会评价等四大部分收集整理了 100 多项具体考核内容的相关材料，经过协会自评、登记主管单位初评、专家组材料审核、实地检查、评估委员会终审等环节，最终获评为 AAAA 级社团组织。这一殊荣标志着协会在规范化建设、服务能力和社会影响力等方面达到了新的高度。

一直以来，协会在主管部门的指导下，秉持遵守宪法、法律、法规和国家政策，践行社会主义核心价值观，遵守社会道德风尚；根据武汉市信息化建设发展的需要，贯彻执行国家的有关法律、法规和政策；以服务社会和服务会员为宗旨，发挥政府管理部门与信息系统用户之间的桥梁和纽带作用；协助管理机关规范和加强系统安全保护工作的管理，协助维护我市网络系统的安全和稳定；推动网络安全技术的发展，促进信息网络用户的法治和安全意识的提高，保障我市信息化建设的健康发展。

此次被评为 AAAA 社会组织，既是对过去工作的肯定，也是对未来发展的激励。协会将以此为新起点，继续发挥自身优势，不断提升服务质量和水平，为行业发展和社会进步做出更大的贡献。

相信在民政及主管部门的指导下，在协会全体成员的共同努力下，武汉市网络安全协会必将在未来的征程中再创辉煌，书写更加灿烂的篇章。

网络安全应用场景供需对接会（智能网联汽车及智能制造专场）在国家网安基地举行

为切实落实市委市政府工作部署，积极促进全市网络安全生态开放和产业发展，针对性推动和支持重点行业重要领域《党委（党组）网络安全工作责任制实施办法》落实，推进在汉车企及智能制造企业进一步做实网络安全工作。10 月 12 日，在省委网信办、市委网信办、市公安局、市经济和信息化局、市交通运输局共同指导下，东风汽车集团有限公司、网络和数据安全全国产才融合中心大力支持下，由国家网络安全人才与创新基地主办，武汉市网络安全协会和武汉企业信息化促进会承办的 2024 武汉市网络安全应用场景供需对接会智能网联汽车及智能制造专场活动在国家网安基地举行，在汉车企及上下游生产企业、智能制造企业、头部网络安全企业、相关高校等近百家单位参加活动，广泛交流并开展供需对接。

在当今科技迅猛发展的时代，智能网联汽车与智能制造已成为驱动经济增长和社会进步的重要引擎。随着汽车电动化、网联化、智能化交融发展，智能网联汽车面临的来自云、路、网等多种路径的网络攻击愈发多元，安全需求愈发强烈。对此，参会企业纷纷提出解决思路，深化与在汉车企和智能制造企业的合作，

共同推动网络安全技术与应用场景的深度融合，搭建产学研用的交流合作平台。

活动中，武汉市公安局网络安全保卫支队大队长孙灯安作以“网络安全法规分析和防护措施”为主题的政策宣讲。武汉大学国家网络安全学院教授、武汉大学信息中心副主任曹越带来以“网联智能车辆中基于云车协同和深度学习的入侵检测机制研究”为题的学术报告。岚图汽车网络安全负责人刘翀分享了岚图汽车网络及数据安全建设历程。

天融信、神州绿盟、奇安信、安恒信息、曙光网络等 34 家知名网络安全企业参展。神龙汽车、岚图汽车科技、东风本田、东风商用车、东风猛士汽车、东风汽车股份、易捷特新能源汽车、扬子江汽车等十余家汽车主机厂数字化部门负责人和来自中汽研 (武汉) 公司、武汉车网智联测试运营公司、武汉极目智能技术公司、黑芝麻智能科技公司等汽车上下游相关企业的负责人受邀出席活动，在展区和路演厅详细了解各网安企业提供的智能网联汽车和智能制造网络安全方面的优秀产品和解决方案。

本次活动紧密围绕智能网联汽车与智能制造领域的网络安全问题和需求开展深入交流，对接资源配置，加强信息交流，实现供需两端协同发力，探索建立长效应用场景供需对接机制。网络安全应用场景供需对接会已成功举办 4 场，400 余家企事业单位深入对接交流、共谋合作发展，实现跨区交流、多产联动，推动网络和数据安全、大数据等先进技术示范应用，赋能产业升级。

我会受邀赴多家单位开展网络安全专题讲座

近日，武汉市网络安全协会党支部书记、秘书长、高级工程师刘悦恒受邀分别为武汉大学、湖北大学、武汉信息职业传播技术学院、湖北盐业集团、鄂北地区水资源配置工程建设与管理局（筹）和武汉文明网开展了一系列网络安全宣传专题讲座。

在武汉大学、湖北大学、武汉信息职业传播技术学院的高校专题讲座中，刘秘书长以《网络安全形势和技术趋势展望》为主题为学子们剖析了网络安全行业的发展动态与未来趋势。通过生动的案例和详实的数据，展示了网络安全在当今数字化时代的关键地位，深入分析了当前复杂多变的网络安全形势，指出了面临的挑战与机遇。同时，他对网络安全技术的未来发展趋势进行了前瞻性的展望，为学子们指明了学习和努力的方向。

在湖北盐业集团、鄂北地区水资源配置工程建设与管理局（筹）、武汉文明网的企事业单位专题讲座中，

刘秘书长以《坚定意识形态自觉，筑牢网络安全防线》为主题，分析新时代意识形态发展新形势。他通过实际案例，阐述了网络安全不仅是技术问题，更是涉及到国家安全、社会稳定和个人权益的重大问题。强调新时代企业人员要增强国家安全意识，提升自我安全素养，树立正确的网络安全观、规范网络行为和提高网络安全意识。

我会将网络安全宣传教育工作继续深入开展，促进我市信息网络用户的法制观念和安全意识的提高，保障我市信息化建设的健康发展。

武汉网安协会共同发起的中国网络空间安全协会智能网联安全专业委员会正式成立

11 月 9 日上午，中国网络空间安全协会智能网联安全专业委员会（以下简称“专委会”）成立大会在湖北省武汉市召开。会议宣读了中央网信办关于同意设立智能网联安全专委会及主任委员人选的决定，提名并表决专委会副主任委员、秘书长、副秘书长人选，审议通过专委会工作规则及 2024-2025 年工作计划。协会理事长，中央网信办网络安全协调局、网络数据管理局主要负责同志出席会议并讲话。

协会理事长指出，专委会要着眼新技术、新应用带来的挑战开展研究，及时向主管部门反馈研究成果及发展中面临的问题，积极支撑政策制定，助力行业形成广泛共识；要充分发挥专家智库作用，加速推动智能网联汽车、无人机、工业控制等领域网络与数据安全能力提升。

中央网信办网络安全协调局、网络数据管理局主要负责同志对专委会的成立表示祝贺，希望专委会能够充分发挥自身优势，为我国的智能网联安全事业作出积极贡献。专委会由华中科技大学、国家互联网应急中心、东风汽车、华为、小米、海尔等 53 家会员单位发起，旨在发挥桥梁纽带作用，组织动员会员单位开展智能网联安全政策法规研讨、标准开发、技术创新、产业协作、智库建设、人才培养、国际交流等工作。

我会作为该专委会发起单位之一，将积极发挥武汉网络安全产业优势，结合我市经济工作重点，积极对接地方主管部门政策资源，为专委会各项工作提供全方位支持，贡献武汉网安力量。


证书

智能网联安全专业委员会

Intelligent Connectivity Security Professional Committee

成员单位

武汉市网络安全协会

网络安全产才融合闭门研讨会成功举办

2024 黄鹤网络安全技术大会分论坛——网络安全产才融合闭门研讨会于 11 月 11 日成功举办，吸引了政府、高校、及企业多方 40 余人共同参与研讨。本次研讨会由黄鹤实验室主办、武汉云计算科技有限公司及奇安信科技集团股份有限公司承办，武汉市网络安全协会、网络和数据安全全国产才融合中心支持，多方参与聚焦网络安全产业发展与人才培养，共同落实国家网络安全相关要求，推动网络安全领域多方深度合作。会议由我会秘书长刘悦恒和工信部人才交流中心武汉办主任严功望共同主持。

武汉临空港经开区现代服务产业办相关负责人在致辞中明确了研讨会的重要意义，为网络安全产业发展和人才培养指明方向。她强调各方应积极协同，形成合力，共同推动网络安全产业蓬勃发展，培养更多优秀人才，为网络安全事业筑牢根基。

在主题分享环节，网安大学筹建办相关负责人深入解读了网络安全态势及网络强国战略。他指出，当前网络安全形势严峻复杂，网络强国战略意义重大，各方需从战略高度重视网络安全工作，加大投入，提升网络安全防护能力，以应对不断涌现的新威胁。湖北大学网络空间安全学院副院长何鹏分享了“三化”融通培养网络安全人才的经验，他提出的“三化”融通人才培养模式，为应对新形势下网络安全挑战提供新的思路与方法，强调在实际工作中要持续探索创新人才培养模式，以适应快速发展的网络安全需求。奇安信集团高校合作中心总监李向辉探讨了网络安全实战人才培养与深度产教融合，通过实际案例展示了产教融合在实战人才培养中的关键作用，强调企业与高校紧密合作的必要性，提出了崭新的校企合作模式，共同培养出契合市场需求的实战型网安人才。黄鹤网络安全实验室技术专家丁勇阐述了安全测评对数字中国建设的保驾护航作用，让与会者了解到安全测评在数字中国建设中的重要地位，为相关工作提供有益的参考。

交流环节中，武汉市数据局相关负责人从政府部门角度出发，介绍了武汉市在数据产业发展和人才需求方面的情况，介绍了武汉市有关政策，对与会单位在数据安全和产业发展方面提出了相关建议和期望。南京嘉环及智网安云负责人从行业整体发展分析网络安全人才培养现状与趋势，提出了各单位应加强行业协作、共享情报资源、共育网安人才的殷切期盼。互动交流环节，与会嘉宾围绕网络安全产才融合展开热烈讨论，共同探索最佳实践路径。

本次研讨会成果丰硕，为各方搭建了坚实的合作交流平台。展望未来，随着我国网络安全形势的不断演变，网安领域的产才融合将在多方面持续深化。相信在各方共同努力下，网络安全产才融合将不断迈上新台阶，为网络安全事业的蓬勃发展注入源源不断的动力。

网联汽车筑安全基石，湖北智研启未来新程

12 月 1 日，智能网联汽车网络安全湖北省工程研究中心首届技术委员会年会暨车联网安全研讨会在湖北大学举行。来自浙江大学、武汉大学、华中科技大学、深圳开源互联网安全技术有限公司、天融信科技集团股份有限公司、岚图汽车科技有限公司、武汉市网络安全协会智能汽车网络安全专委会等单位的专家学者参加会议。

湖北大学副校长曾祥勇在致辞中，对专家学者们的到来表示欢迎和感谢。他表示，湖北大学作为工程研究中心牵头单位，将携手各成员单位，整合优化资源，紧密聚焦智能网联汽车网络安全的基础理论、前沿检测技术以及高效防护策略等核心关键技术，坚持以“用”为导向，开展持续而深入的探索与研究，助推我省“车谷、网谷”科技创新大走廊发展。

会上，湖北大学科学技术发展研究院负责人宣读了工程研究中心技术委员会名单，曾祥勇为技术委员会委员颁发聘书。工程研究中心主任、网络空间安全学院院长李念教授作了年度建设进展报告。专家学者们就工程研究中心发展规划和研究方向提出了意见和建议。技术委员会主任、武汉大学教授何德彪表示，将与全体委员携手合作，共同为智能网联汽车网络安全发展贡献力量。

据悉，智能网联汽车网络安全湖北省工程研究中心瞄准智能网联汽车与网络安全领域技术创新，力争取得更多突破性成果，为社会经济发展作出更大贡献。

科技高质量发展风险管理与保险论坛在武汉成功举办

12 月 12 日，“科技高质量发展风险管理与保险论坛”在武汉会议中心成功举办。来自武汉市政府部门、科技企业、行业协会、保险机构 100 多位人员参加会议。

会议以“科技 + 金融、共创新未来”为主题，武汉大学经济与管理学院副院长罗知、湖北省高新技术发展促进中心副主任孟凡宝、武汉市网络安全协会秘书长刘悦恒等专家，就中国经济形势发展与机遇、湖北省科技金融探索与实践、网络安全形势分析与展望、知识产权助力企业创新发展、企业信用风险管理、金融机构运营风险管理、科技保险等话题进行探讨。

武汉市地方金融管理局相关负责人表示，2007 年，科技部、保监会联合印发《关于确定第一批科技保险创新试点城市的通知》，武汉市被评为第一批科技保险创新试点城市。2020 年，武汉市东湖高新区又获批全国科技保险创新示范区。近年来，武汉市金融局在持续优化营商环境，支持各类保险机构开展科技保险业务，推动武汉市科技创新取得新突破。

论坛上，江泰保险经纪公司、武汉市网络安全协会网络安全保险工作委员会、武汉华康科技有限公司签订网络安全保险项目合作协议。长江千机 (武汉) 文旅科技公司、武汉北斗产业创新中心公司、食安康（湖北）科技公司与江泰保险经纪公司签订保险经纪服务委托协议。

“创新驱动，安全护航”
2024 年“黄鹤杯”网络安全人才创新大赛成功举办

12 月 19 日，备受瞩目的 2024 年“黄鹤杯”网络安全人才创新大赛决赛在国家网安基地盛大举行，这场以“创新驱动，安全护航”为主题的赛事，犹如一场网络安全领域的智慧盛宴，吸引了来自全国各地网络安全企业、高校以及众多专业人士的广泛参与，成功搭建起推动网络安全技术创新和产业发展的重要平台。

本次大赛由国家网安基地主办，武汉市网络安全协会承办，网络和数据安全全国产才融合中心、武汉网络安全技术有限公司、武汉攀升鼎承科技有限公司、小米安全中心共同协办。自 2018 年举办以来，“黄鹤杯”已成为全国网络安全领域极具影响力的专业品牌赛事。今年的大赛紧密贴合时代发展脉搏，深度聚焦网络安全前沿趋势，精心设置了网络安全理论创新赛和实践创新赛两个赛道，申报成果广泛涉及人工智能、5G+ 工业互联网、数据隐私、生态安全、能源安全等多个专业和行业领域，共收到 53 项成果报名，经过初赛的激烈角逐，32 项成果脱颖而出入围决赛。

决赛现场，各参赛团队全力以赴，通过精彩的路演答辩展示其在网络安全领域的创新成果。十位评审专家和五十位大众评审员秉持专业、严谨的态度，从创新性、科学性、技术水平、应用价值等多个维度进行严格评审。最终，神州绿盟武汉科技有限公司的“云上数据泄露风险侦察技术”凭借其卓越的创新与应用价值，荣获实践创新赛一等奖；华中科技大学 CPSS 战队的“智慧交通物联网数据协同异常检测方法”则在理论创新赛中拔得头筹。此外，大赛还评选出多个二等奖、三等奖以及各类专项奖项，对在不同方面表现出色的团队和个人予以表彰。

此次大赛成果斐然。例如，武汉大学国家网络安全学院 ASAP 课题组提出的“基于群决策的共识自适应信任管理关键技术”，构建了全新的信任管理模式，为网络安全信任管理提供了新的方向；中国电信股份有限公司武汉分公司的“电子政务外网安全防护解决方案”，有效保障了政务数据安全，有力推动了电子政务的稳健发展；小米科技（武汉）有限公司的“人车家生态安全左移”项目，显著提升了智能交通场景的安全性，为智能交通生态的安全保障贡献了创新力量；华康科技编制的《网络安全风险量化评估规范》团体标准，为

各类机构快速、科学地评估网络安全风险，直观了解自身安全水平提供了专业的方法指引。这些成果不仅彰显了参赛团队的高超技术水平，更为网络安全技术产业发展注入了新的活力与智慧源泉。

大赛的成功举办，离不开各方的齐心协力。武汉市网络安全协会秘书长刘悦恒表示，“黄鹤杯”将继续依托国家网安基地的平台资源优势，为网络安全人才和企业创造更为广阔的发展空间。本次大赛专家组对参赛选手的精彩表现给予高度评价，认为他们的实践成果在技术创新、技术突破、应用创新和功能创新等方面都取得了显著成绩，理论成果中提出了许多具有前瞻性和创新性的理论成果，展现了网络安全领域深厚的学术底蕴和蓬勃的创新活力。专家们殷切期望各团队能够持续发挥自身优势，为网络安全事业添砖加瓦，做出更大贡献。

此次大赛的圆满落幕，进一步推动了网络安全领域的技术创新和人才培养，为我国网络安全事业发展注入了新的强大动力。展望未来，“黄鹤杯”将继续发挥品牌赛事的深远影响力，持续促进网络安全产业的高质量发展，引领网络安全领域迈向新的辉煌。







附：2024 年“黄鹤杯”网络安全人才创新大赛获奖名单

理论赛获奖名单	实践赛获奖名单
一等奖：（1名）	**一等奖：（1名）**
获奖团队：CPSS战队（孙思宇、邓云康、徐良松、朱苏文、秦书琪、王帅） 获奖成果：《智慧交通物联网数据协同异常检测方法》	获奖团队：神州绿盟武汉科技有限公司 获奖成果：《云上数据泄露风险侦察技术》
二等奖：（2名）	**二等奖：（2名）**
获奖团队：武汉华康科技有限公司 获奖成果：《网络安全风险量化评估规范》	获奖团队：中国电信股份有限公司武汉分公司 获奖成果：《电子政务外网安全防护解决方案》
获奖团队：国网武汉供电公司信息通信分公司 获奖成果：《基于区块链的电力应用数据安全共享研究》	获奖团队：广州赛讯信息技术有限公司 获奖成果：《5G 网络下基于零信任浏览器的数据安全访问方案》
三等奖：（3名）	**三等奖：（3名）**
获奖团队：武汉大学国家网络安全学院ASAP课题组 获奖成果：《基于群决策的共识自适应信任管理关键技术》	获奖团队：深圳万物安全科技有限公司 获奖成果：《基于云原生和AI打造物联网数据安全大脑》
获奖团队：张明武、张媛媛、王玉珠、沈华 获奖成果：《群智感知的数据安全保护机制研究》	获奖团队：武汉安恒信息科技有限公司 获奖成果：《AiLand数据安全岛隐私计算平台》
获奖团队：杨子旭、王依婷、赵诗语、秦灏阳、裴昊天、胡林 获奖成果：《基于改进YOLOv9的智能网联汽车图像脱敏系统》	获奖团队：湖北生物科技职业学院 获奖成果：《虚拟仿真教学平台》
理论创新突破奖：（1名）	**实践创新突破奖：（1名）**
获奖团队：李荣及该标准编制组 获奖成果：《湖北省重要网络和信息系统密码应用技术指南》	获奖团队：湖北天融信网络安全技术有限公司 获奖成果：《基于整车在环的车联网信息安全检测平台》
理论前沿探索奖：（1名）	**实践行业推动奖：（1名）**
获奖团队：智网安云（武汉）信息技术有限公司 获奖成果：《制造业数据安全管理中的数据分类分级方法指南》	获奖团队：小米科技（武汉）有限公司 获奖成果：《人车家生态安全左移》
理论价值学术奖：（1名）	**实践价值效益奖：（1名）**
获奖团队：张帆、孙宝林、刘小丽、罗良逸 获奖成果：《一种新的信息流安全模型及其分析和验证方法》	获奖团队：华中师范大学信息化办公室 获奖成果：《网络安全工作管理平台V1.0》
所有晋级决赛的参赛队全部获得本次大赛优胜奖	所有晋级决赛的参赛队全部获得本次大赛优胜奖

武汉市网络安全协会服务指南

一 移动应用安全公益检测服务

依托由我会主办的全国首个“移动应用安全公益检测平台”，向广大会员提供移动应用安全公益检测服务。

二 网络安全等级保护测评

依托我会各专业网络安全等级保护测评机构，向广大会员提供网络安全等级保护测评服务。

三 网络安全保险服务

我会与武汉东湖科技保险发展促进中心共建的“东湖网络安全保险服务中心”，提供网络安全保险有关安全服务。依托我会专家库及专业会员力量，协会设立了“数字资产网络安全风险量化实验室”，为我市各类型机构提供风险量化评估服务。

四 网络安全相关标准制定服务

我会是全国团体标准信息平台注册发布单位，具有全国团体标准发布资格，并与全国信息安全标准化技术委员会建立了长期合作关系。我会依据国家法规政策与地方发展需要，根据市场需求，可为各会员单位提供各类网络安全相关标准化制定、发布与推广服务。

五 资质认证

1、ISO 体系类
2、CCRC 信息安全服务资质
3、ITSS 运维服务能力评估
4、CS 信息系统建设及服务能力评估
5、CMMI 软件研发能力成熟度
6、DCMM 数据管理能力成熟度
7、知识产权
8、软件测试

六 人才服务

1、网络信息安全技能培训及认证
2、网络信息安全师资培训及认证
3、CISP 注册信息安全专业人员
4、CISSP（ISC）^{2} 注册信息系统安全师
5、CCSSP 国际注册云安全系统认证专家
6、CISM 注册信息安全经理
7、CSSLP（ISC）^{2} 注册软件生命周期安全师
8、中级高级职称
9、八大员
10、承接类定制专业网络安全培养培训工作

七 咨询服务

我会建有拥有全市最大最全的网络安全高级专家智库，长期为各级主管部门提供智力支撑。可承接网络安全领域各类的课题研究、政策与法律咨询工作。

八 网络安全宣传与会务服务

我会长期参与组织历年省市“国家网络安全宣传周”系列宣传活动，主办承办了各类各级别专业性论坛、赛事等大型活动。拥有丰富的活动策划与组织经验和专业团队。

武汉市网络安全协会入会指南

在武汉市委网信办主管下，作为唯一代表全市网络安全产业的专业性社团法人，“武汉市网络安全协会”积极发挥好政府与企业间的桥梁纽带作用，全面推进全市网络安全工作，服务网安各领域企事业单位，得到了主管部门和广大网安企业的广泛认可。

武汉网安协会将继续规范办会，以服务会员为中心，积极谋划主动作为，带动上下游产业链，开展形式多样的学习交流等活动，协助主管部门推动全市网络安全与信息化建设，向全国推介“武汉网络安全”集体品牌，助力武汉网络产业健康发展。

为了更好地发挥协会职能，凝聚更多的网络安全优秀企事业单位，我会诚邀贵单位积极加入到“武汉网络安全”的大家庭中来，凝心聚力，共谋产业升级，助力武汉崛起，为武汉网络安全产业健康发展贡献我们的集体智慧和力量！

入会基本条件

依据我会《章程》规定，我会会员分为单位会员和个人会员，入会基本条件如下：

一、在武汉市注册的企事业法人单位、具有武汉市户籍或长期居住的专业人士。

外地企业在汉分公司或办事处机构，需提交驻汉相关证明，协会需实地考察实际经营情况，非武汉户籍个人入会需提供本地工作或长期居住证明。

二、从事以下某项或多项领域的单位和专业人士：

1. 物理安全：环境安全（灾备防护等）、设备安全（设备防毁、电磁屏蔽、防电磁干扰等）、介质安全（介质数据安全等）；

2. 主机安全：身份识别（电子 / 生物信息鉴 别）、主机防护（可信计算、入侵检测、访问控制等）、防恶意代码（病毒防治等）、操作系统安全；

3. 网络安全：通信安全（通信鉴权、保密等）、网络监测（入侵检测、网络监测）；

4. 边界安全：内容安全（内容过滤与控制、防泄漏）边界安全、边界隔离、入侵防范、边界访问控制（防火墙、安全路由器等、网络终端安全（接入控制等）

5. 应用安全：应用服务安全、应用服务安全支持；

6. 数据安全：数据平台安全（安全数据库、数据库安全部件等）、备份与恢复；

7. 安全管理与支持：综合审计、应急响应支持、密码支持（密钥管理）、风险评估、安全管理（安全产品管理平台、安全监控等）、等保测评、网络安全运行维护；

8. 工业信息安全：应用工业互联网的工业企业、工业互联网平台企业、工业互联网基础设施运营企业及专业人士；

9. 从事网络安全和信息化领域相关的信息系统集成、运维服务、科学研究、检验检测、评价评估、人才培养、法律服务、金融服务等方面的专业机构及专业人士；

10. 在网络安全和信息化产业链上下游关系紧密的有关机构和专业人士。

三、单位会员在武汉市有实际经营的独立办公场所，开展正常经营活动超过一年以上时间。个人会员在武汉市从事本专业领域工作超过一年以上时间。

四、单位或个人信用良好，经“信用中国”等国家各级信用平台查询，无违法违规记录。

五、单位会员有专业从事网络信息安全领域的技术人员，个人会员有从事本专业的技术能力并提供相关证明材料。

六、同意协会《章程》，支持并拥护协会相关《公约》、《倡议》、《团体标准》，积极参加协会活动，愿为武汉网络安全产业发展贡献自己力量。

入会流程

一 申请人填写《武汉市网络安全协会入会申请表》提交协会；

二 协会进行入会资格审核；

三 符合入会条件，协会核发《入会通知书》；

四 申请单位或个人按要求提交纸质版材料 1 份，并按规定标准缴纳会费；

五 会籍资料存档，协会颁发会员证书或标牌并公示；

入会联系人：张玉萍　　联系电话：027-82757716　　https://www.whcsa.org.cn

WHCSA
武汉市网络安全协会
WUHAN CYBER SECURITY ASSOCIATION

没有网络安全　就没有国家安全

There is no national security without network security.

公众号二维码

视频号二维码

地址：武汉市江汉区发展大道 164 号武汉科技大厦 6 楼 605
电话：027—82757716　网址：www.whcsa.org.cn　邮箱 :hz@whcsa.org.cn