武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2024年第1期　总第3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

孙智书法作品

网络安全，是当下的热词。它是国家必须高度重视的问题，更是全社会与全体成员面临的严峻挑战。

说起暴雨、洪水、火灾、交通事故，人们脑海里就会浮现出电影般的画面，但说起网络风险，人们可能就没有这种形象、真切的感受。这种对网络风险的感受，淡化了人们对网络风险的认识，也弱化了人们对网络安全的重视。网络风险在哪里？它就在你我身边，如影随形。因为在互联网时代，特别是互联网手机的普及，已将人们的活动与互联网绑在一起，人已成为互联网的一部分，成为“网中人”。网络风险涉及我们每一个人，谁能置身“网”外，独善其身？

互联网虽然是一个虚拟的世界，但它却是一个现实的存在。社会巨大的财富在网中运动或创造，人们的许多活动通过网络进行。网络在给我们带来财富、便捷、高效的同时，也给我们带来了各种风险，如网络攻击、信息泄露、业务中断、恶意软件、敲诈勒索等。当你的手机上绑定你的银行卡，你的银行存款就是你的网络风险；当企业实现数字化、智能化时，它的生产就有了网络风险。网络风险对人们的财富与活动构成极大的破坏性及损害性影响。

网络风险有以下特征：一是广泛性。随着互联网的普及和广泛运用，网络风险涉及政治、军事、经济、文化、生活等领域，无处不在，无人不有。网络风险已是人类第一大风险。二是多样性。网络风险来自多种途径，手段多种多样，风险呈多样化趋势。三是无形性。网络风险是借助无形的信息手段产生，隐藏在人类一切互联网活动之中，不像暴雨、洪水、火灾，看得见，感受得到。四是难测性。风险无法预测，暴雨、暴风可以预测，网络风险什么时间发生？风险源在哪里？以什么方式产生？损失有多大？难以预测。五是难控性。网络风险技术复杂，加上人为因素，导致风险控制与化解难度大。六是系统性。网络是一个庞大的系统，一个节点受到破坏，将会导致使用者整个网络的瘫痪。七是人为性。网络风险的制造者是人，是人的违法行为、不道德行为或疏忽行为产生的。

防范网络风险，强化网络安全，是社会每个组织和个人的重要任务，它不仅关乎国家的整体安全，也与每个人的切身利益紧密相关。在网络安全工作中，我们主要应做好以下三点：一是提高风险防范意识，二是加强风险防范管理，三是用保险方式解决经济损失补偿问题。

武汉市网络安全协会网络安全保险工作委员会主任、
武汉东湖科技保险发展促进中心主任：孙智

目 录

CATALOGUE

标准化工作

协会动态

新增会员

工业和信息化部关于印发《工业领域数据安全能力提升实施方案（2024-2026 年）》的通知

各省、自治区、直辖市、计划单列市及新疆生产建设兵团工业和信息化主管部门，有关行业协会，有关企业，部属有关单位，部属各高校：

现将《工业领域数据安全能力提升实施方案（2024-2026 年）》印发给你们，请认真抓好贯彻落实。

工业和信息化部

2024 年 2 月 23 日

工业领域数据安全能力提升实施方案（2024-2026 年）

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通等各环节，保障数据安全，事关国家安全大局。为贯彻落实习近平总书记关于数据安全的重要指示精神和党中央、国务院决策部署，推动《中华人民共和国数据安全法》《中华人民共和国网络安全法》《工业和信息化领域数据安全管理办法（试行）》等在工业领域落地实施，加快提升工业领域数据安全保护能力，助力工业高质量发展，夯实新型工业化发展的安全基石，制定本方案。

一、总体要求

（一）指导思想

以习近平新时代中国特色社会主义思想为指导，全面贯彻落实党的二十大精神，坚定不移贯彻总体国家安全观，坚持统筹发展和安全，坚持底线思维和极限思维，坚持目标导向和问题导向，以构建完善工业领域数据安全保障体系为主线，以落实企业主体责任为核心，以保护重要数据，提升监管能力、强化产业支撑等为重点，提高数据安全治理能力，促进数据要素安全有序流动和价值释放，为加快推进新型工业化，建设制造强国、网络强国和数字中国提供坚实支撑。

（二）基本原则

统筹推进，重点突破。加强顶层谋划，系统推进数据安全组织架构、政策制度、管理机制、标准规范、技术手段建设和产业发展工作。以强化重点行业、重点企业、重要系统平台、重要数据保护为切入点，以点带面促进整体保护水平提升。

政府引导，协同共治。综合运用正向激励和反向

约束等方式，选树标杆典型，强化监管执法，压实企业主体责任。充分发挥行业协会、龙头企业、专业机构、高等院校等各方力量，形成数据安全协同治理的良好局面。

场景牵引，分业施策。摸清数据处理重点环节风险易发场景的特点规律，紧贴业务场景数据保护需求，强化科学防控 . 结合行业特色、数据特征等，差异化指导、精准化施策，加速提升行业数据安全管理水平。

创新驱动，技管结合。不断创新管理模式、技术、产品与服务，适应新时期工业领域数据安全保护新形势、新特点和新需求。注重“以技管数”手段建设和运用，与日常监管形成合力。

（三）总体目标

到 2026 年底，工业领域数据安全保障体系基本建立。数据安全保护意识普遍提高，重点企业数据安全主体责任落实到位，重点场景数据保护水平大幅提升，重大风险得到有效防控。数据安全政策标准、工作机制、监管队伍和技术手段更加健全。数据安全技术、产品、服务和人才等产业支撑能力稳步提升。

——基本实现各工业行业规上企业数据安全要求宣贯全覆盖。

——开展数据分类分级保护的企业超 4.5 万家，至少覆盖年营收在各省（区、市）行业排名前 10% 的规上工业企业。

——立项研制数据安全国家、行业、团体等标准规范不少于 100 项。——遴选数据安全典型案例不少于 200 个，覆盖行业不少于 10 个。

——数据安全培训覆盖 3 万人次，培养工业数据安全人才超 5000 人。

二、重点任务

（一）提升工业企业数据保护能力

1. 增强数据安全保护意识。加大数据安全法律法规和整策标准宣贯培训力度，提高各行业企业数据安全意识。督促企业依法依规落实数据安全主体责任，压实各单位法定代表人或主要负责人数据安全第一责任，建立健全数据安全管理体系和工作机制，配足数据安全岗位和人员队伍，定期开展数据安全教育培训。引导企业贯彻发展与安全并重原则，将数据安全管理要求融入本单位发展战略和考核机制，加强数据安全工

专栏 1　数据安全保护筑基工程

1.夯实数据分类分级基础。分行业分领域研究制定重要数据和核心数据识别细则，形成“1+N”的工业领域数据分类分级规范体系，科学指导各行业落地实施。持续迭代重要数据和核心数据目录，逐步摸清行业重要数据规模、分布、处理等情况，明确行业重点保护数据对象。

2.编制数据保护实践指南。结合重点数据处理场景、典型业务场景、易发频发风险场景等数据安全保护需求和难点，研究制定工业领域数据安全保护实践系列指南，为企业数据保护和风险防范提供实操参考。面向数据出境需求较大的重点行业，分类制定数据出境安全指引，指导企业依法依规开展数据出境安全评估。

3.分业推进数据安全保护能力跃升。在有序推进宣贯培训、分类分级保护等工作基础上，立足钢铁、汽车、纺织、集成电路等行业实际，聚焦重点场景、重点环节、重要系统平台、重要数据等，进一步加强行业数据安全主体责任落实和保护力度，实现行业数据安全保护能力整体跃升。

作与业务发展同谋划、同部署、同落实、同考核。

2. 开展重要数据安全保护。指导企业建立健全数据分类分级保护等安全管理制度，定期梳理识别重要数据和核心数据，形成目录并及时报备。督促重要数据和核心数据处理者明确数据安全负责人和管理机构，落实数据分级防护要求，每年至少开展一次数据安全风险评估，及时发现整改安全隐患，按要求报送评估报告。指导企业加强重要数据和核心数据安全风险监测与应急处置，及时报告重大风险事件。推动各行业企业加强商用密码应用保护数据安全。

3. 强化重点企业数据安全管理。遴选掌握关键核心技术、代表行业发展水平、关系产业链安全稳定或关乎国家安全的企业，滚动编制工业领域数据安全风险防控重点企业名录。将名录内企业作为数据安全监管重点，督促其在落实数据安全要求基础上，着重提升风险监测、态势感知、威胁研判和应急处置等能力。发挥部省两级主管部门作用，统筹各方数据安全监测预警手段和技术力量，加强技术支持，协同做好企业数据安全保护。

4. 深化重点场景数据安全保护。指导企业围绕数据汇聚、共享、出境、委托加工等重点数据处理场景，排查数据安全保护薄弱点，实施贴合行业特点的数据保护措施。聚焦供应链上下游协作、服务外包、上云上平台等典型业务场景，厘清多主体数据安全责任界面和衔接模式，建立全链条全方位数据安全保护体系。针对勒索病毒攻击、漏洞后门、人员违规操作、非受控远程运维等易发频发风险场景，加强风险自查自纠，采取精准的管理和防护措施。面向数据要素大规模流通交易典型场景，打造一批安全解决方案。

（二）提升数据安全监管能力

5. 完善数据安全政策标准。建立健全工业领域数据安全管理制度，推动出台风险评估实施细则、应急预案、行政处罚裁量指引等政策文件。持续完善重要数据识别、备案、分级防护、风险评估等全流程监管机

专栏 2　打造数据安全风险防控品牌

1.“数安护航”专项行动。分行业、分批次集中开展数据安全风险排查和防范，聚焦数据泄露、篡改、滥用、违规传输、非法访问、流量异常等突出风险，利用企业自查、远程检测、现场诊断等手段，针对性增强风险应对处置能力

2.“数安铸盾”应急演练。面向重点行业，模拟勒索病毒攻击、供应链攻击等易发典型数据安全风险事件，组织开展全要素、全流程应急演练，持续优化事件响应流程和机制，锻炼培养一批应急支撑队伍。

专栏 3　数据安全技术保障工程

1.统筹建设工业和信息化领域数据安全管理平台。建立完善工业领域数据安全监测、信息报送与共享、应急管理、安全评估等系统功能，强化风险统一汇集、分析、研判和通报，支撑事件应急处置、辅助决策、跟踪追溯等工作，提供风险评估、出境安全评估、防护能力评估等服务，覆盖不少于20个省级(行业级)节点和500 个企业节点。

2.建立工业领域数据安全工具库。围绕数据分类分级、安全防护、检测评估、合规检查、应急处置、攻击追溯、密码应用等方面，研发一批规范化、便携式的工具，为高效开展数据安全监管和保护工作提供支撑。

制，加强监督检查。组建工业领域网络与数据安全行业标准化组织，发布数据安全标准体系建设指南、加快研制重要数据识别、安全防护、风险评估、产品检测、密码应用等亟需标准。鼓励地方参照制定本地区数据安全政策。

6. 加强数据安全风险防控。完善工业领域数据安全风险信息报送与共享工作机制，组建数据安全风险分析专家组，动态管理风险直报单位库，协同加强地方力量，常态化开展风险监测、报送、预警、处置等工作。摸排数据安全风险事件特点和规律，建立重大风险事件案例库，加强案例剖析和风险提示。面向重点行业开展“数安护航”专项行动，定期组织“数安铸盾”应急演练 , 提升事件快速反应、规范处置、协同联动水平。

7. 推进数据安全技术手段建设。统筹建设工业和信息化领域数据安全管理平台，建立工业领域数据安全工具库，形成集数据资源管理、态势感知、风险信息报送与共享、技术测试验证、事件应急响应等功能于一体的技术能力，加强与网络安全技术、密码技术手段协同。推动有条件的地方、行业、企业等加快建立数据安全风险监测与应急处置等技术手段，强化“部 -

省 - 企业”技术能力三级联动，不断提升技术保障水平。

8. 锻造数据安全监管执法能力。规范数据安全事件调查处置程序，丰富取证方法和手段。加快完善数据安全执法流程和工作机制，推动地方工业和信息化主管部门将数据安全纳入本地区行政执法事项清单，指导各行业、各地方依法严格处置违法行为，加强执法案例宣介与警示教育。建立健全数据安全违法违规行为投诉举报机制，多渠道收集违法违规线索。加大监管执法人员培训力度，推动地方工业和信息化主管部门强化数据安全监管力量，打造专业化、规范化监管执法队伍。

（三）提升数据安全产业支撑能力

9. 加大技术产品和服务供给。加强工业数据智能分类分级、工业数据库审计、低时延加密传输等共性技术优化升级。加大适配工业业务场景和数据特征的轻量级数据加密、隐私计算、密态计算等关键技术攻关。支持使用商用密码技术保障工业领域数据安全。围绕工业数据泄露、窃取、篡改等风险，推动流量异常监测、攻击行为识别、事件追溯和处置等产品研发。加强面向工业云、工业大数据、工业互联网平台等新兴应用的数据安全架构设计。支持工业领域数据安全＂产品 + 服务”供给模式创新

10. 促进应用推广和供需对接。加大多方安全计算、数据防勒索、数据溯源、商用密码等技术产品在工业领域的试点应用。组织遴选一批在各行业具有广泛应用价值的通用数据安全技术和产品，打造一批面向行业、面向场景、面向中小企业的数据安全解决方案，形成一批工业领域数据安全典型案例，分行业、分地区开展宣传推广。推动各行业利用主题沙龙、路演等渠道开展数据安全技术产品和服务供需对接活动。发挥数据安全产业公共服务平台作用，强化信息共享、资源对接等服务。

11. 建立健全人才培养体系。面向不同行业、岗位、层级数据安全工作需求，推动专业化、特色化数据安全教材课程开发，规范化开展职业人才资格认定。支持产学研用各方加强合作，依托培训中心、实训基地、网络学习平台等联合培养复合型管理人才和实战型技能人才，通过技能竞赛、技术交流、学习进修、岗位练兵等形式持续促进人才知识更新和能力提升。鼓励工业企业建立健全数据安全绩效评价机制，加强数据安全人才激励。

三、保障措施

（一）加强组织协调。工业和信息化部加强工作统筹，做好与国家数据安全工作协调机制的衔接。各地工业和信息化主管部门负责组织实施本地区实施方案。鼓励各地结合实际制定细化工作方案，加强与相关部门合作，确保目标任务落实。充分发挥高校、科研院所、第三方机构等在实施方案宣贯、手段建设指导、技术交流合作、成果应用推广等方面的专业作用，引导企业加强数据安全能力建设。

（二）加大资源保障。统筹利用现有资金渠道，加大工业领域数据安全工作投入，支持关键核心技术攻关和公共服务平台建设。深化产融合作，支持数据安全企业参与“科技产业金融一体化”专项，通过国家产融合作平台获得便捷高效的金融服务。鼓励各地将数据安全纳入地方工业领域数字化转型发展相关规划，在支持数字化、网络化、智能化等项目时，同步明确数据安全要求，引导企业在信息化建设中为数据安全防护安排一定比例资金。

（三）强化成效评估。各行业、各地区及时跟踪调度实施方案落实情况，总结经验做法，评估工作成效，加强沟通交流，及时报告重大进展情况或问题。工业和信息化部对工作推动有力、取得明显成效的地区、企业和单位予以表扬，对优秀经验做法加强提炼总结和推广应用。

（四）做好宣传引导。综合利用产业活动、国际合作等方式，宣传普及工业领域数据安全理念和举措，提高地方、企业和公众对工业领域数据安全的认可度。充分调动行业协会、学会、产业联盟等力量，引导企业加强自律、凝聚共识，营造行业数据安全保护良好氛围。

中华人民共和国保守国家秘密法

（1988 年 9 月 5 日第七届全国人民代表大会常务委员会第三次会议通过 2010 年 4 月 29 日第十一届全国人民代表大会常务委员会第十四次会议第一次修订 2024 年 2 月 27 日第十四届全国人民代表大会常务委员会第八次会议第二次修订）

第一章　总则

第一条　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现代化建设事业的顺利进行，根据宪法，制定本法。

第二条　国家秘密是关系国家安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

第三条　坚持中国共产党对保守国家秘密（以下简称保密）工作的领导。中央保密工作领导机构领导全国保密工作，研究制定、指导实施国家保密工作战略和重大方针政策，统筹协调国家保密重大事项和重要工作，推进国家保密法治建设。

第四条　保密工作坚持总体国家安全观，遵循党管保密、依法管理，积极防范、突出重点，技管并重、创新发展的原则，既确保国家秘密安全，又便利信息资源合理利用。

法律、行政法规规定公开的事项，应当依法公开。

第五条　国家秘密受法律保护。

一切国家机关和武装力量、各政党和各人民团体、企业事业组织和其他社会组织以及公民都有保密的义务。

任何危害国家秘密安全的行为，都必须受到法律追究。

第六条　国家保密行政管理部门主管全国的保密工作。县级以上地方各级保密行政管理部门主管本行政区域的保密工作。

第七条　国家机关和涉及国家秘密的单位（以下简称机关、单位）管理本机关和本单位的保密工作。

中央国家机关在其职权范围内管理或者指导本系统的保密工作。

第八条　机关、单位应当实行保密工作责任制，依法设置保密工作机构或者指定专人负责保密工作，健全保密管理制度，完善保密防护措施，开展保密宣传教育，加强保密监督检查。

第九条　国家采取多种形式加强保密宣传教育，将保密教育纳入国民教育体系和公务员教育培训体系，鼓励大众传播媒介面向社会进行保密宣传教育，普及保密知识，宣传保密法治，增强全社会的保密意识。

第十条　国家鼓励和支持保密科学技术研究和应用，提升自主创新能力，依法保护保密领域的知识产权。

第十一条　县级以上人民政府应当将保密工作纳入本级国民经济和社会发展规划，所需经费列入本级预算。

机关、单位开展保密工作所需经费应当列入本机关、本单位年度预算或者年度收支计划。

第十二条　国家加强保密人才培养和队伍建设，完善相关激励保障机制。

对在保守、保护国家秘密工作中做出突出贡献的

组织和个人，按照国家有关规定给予表彰和奖励。

第二章　国家秘密的范围和密级

第十三条　下列涉及国家安全和利益的事项，泄露后可能损害国家在政治、经济、国防、外交等领域的安全和利益的，应当确定为国家秘密：

（一）国家事务重大决策中的秘密事项；

（二）国防建设和武装力量活动中的秘密事项；

（三）外交和外事活动中的秘密事项以及对外承担保密义务的秘密事项；

（四）国民经济和社会发展中的秘密事项；

（五）科学技术中的秘密事项；

（六）维护国家安全活动和追查刑事犯罪中的秘密事项；

（七）经国家保密行政管理部门确定的其他秘密事项。

政党的秘密事项中符合前款规定的，属于国家秘密。

第十四条　国家秘密的密级分为绝密、机密、秘密三级。

绝密级国家秘密是最重要的国家秘密，泄露会使国家安全和利益遭受特别严重的损害；机密级国家秘密是重要的国家秘密，泄露会使国家安全和利益遭受严重的损害；秘密级国家秘密是一般的国家秘密，泄露会使国家安全和利益遭受损害。

第十五条　国家秘密及其密级的具体范围（以下简称保密事项范围），由国家保密行政管理部门单独或者会同有关中央国家机关规定。

军事方面的保密事项范围，由中央军事委员会规定。

保密事项范围的确定应当遵循必要、合理原则，科学论证评估，并根据情况变化及时调整。保密事项范围的规定应当在有关范围内公布。

第十六条　机关、单位主要负责人及其指定的人员为定密责任人，负责本机关、本单位的国家秘密确定、变更和解除工作。

机关、单位确定、变更和解除本机关、本单位的国家秘密，应当由承办人提出具体意见，经定密责任人审核批准。

第十七条　确定国家秘密的密级，应当遵守定密

权限。

中央国家机关、省级机关及其授权的机关、单位可以确定绝密级、机密级和秘密级国家秘密；设区的市级机关及其授权的机关、单位可以确定机密级和秘密级国家秘密；特殊情况下无法按照上述规定授权定密的，国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门可以授予机关、单位定密权限。具体的定密权限、授权范围由国家保密行政管理部门规定。

下级机关、单位认为本机关、本单位产生的有关定密事项属于上级机关、单位的定密权限，应当先行采取保密措施，并立即报请上级机关、单位确定；没有上级机关、单位的，应当立即提请有相应定密权限的业务主管部门或者保密行政管理部门确定。

公安机关、国家安全机关在其工作范围内按照规定的权限确定国家秘密的密级。

第十八条 机关、单位执行上级确定的国家秘密事项或者办理其他机关、单位确定的国家秘密事项，需要派生定密的，应当根据所执行、办理的国家秘密事项的密级确定。

第十九条 机关、单位对所产生的国家秘密事项，应当按照保密事项范围的规定确定密级，同时确定保密期限和知悉范围；有条件的可以标注密点。

第二十条 国家秘密的保密期限，应当根据事项的性质和特点，按照维护国家安全和利益的需要，限定在必要的期限内；不能确定期限的，应当确定解密的条件。

国家秘密的保密期限，除另有规定外，绝密级不超过三十年，机密级不超过二十年，秘密级不超过十年。

机关、单位应当根据工作需要，确定具体的保密期限、解密时间或者解密条件。

机关、单位对在决定和处理有关事项工作过程中确定需要保密的事项，根据工作需要决定公开的，正式公布时即视为解密。

第二十一条 国家秘密的知悉范围，应当根据工作需要限定在最小范围。

国家秘密的知悉范围能够限定到具体人员的，限定到具体人员；不能限定到具体人员的，限定到机关、单位，由该机关、单位限定到具体人员。

国家秘密的知悉范围以外的人员，因工作需要知悉国家秘密的，应当经过机关、单位主要负责人或者其指定的人员批准。原定密机关、单位对扩大国家秘密的知悉范围有明确规定的，应当遵守其规定。

第二十二条 机关、单位对承载国家秘密的纸介质、光介质、电磁介质等载体（以下简称国家秘密载体）以及属于国家秘密的设备、产品，应当作出国家秘密标志。

涉及国家秘密的电子文件应当按照国家有关规定作出国家秘密标志。

不属于国家秘密的，不得作出国家秘密标志。

第二十三条 国家秘密的密级、保密期限和知悉范围，应当根据情况变化及时变更。国家秘密的密级、保密期限和知悉范围的变更，由原定密机关、单位决定，也可以由其上级机关决定。

国家秘密的密级、保密期限和知悉范围变更的，应当及时书面通知知悉范围内的机关、单位或者人员。

第二十四条 机关、单位应当每年审核所确定的国家秘密。

国家秘密的保密期限已满的，自行解密。在保密期限内因保密事项范围调整不再作为国家秘密，或者公开后不会损害国家安全和利益，不需要继续保密的，应当及时解密；需要延长保密期限的，应当在原保密期限届满前重新确定密级、保密期限和知悉范围。提前解密或者延长保密期限的，由原定密机关、单位决定，也可以由其上级机关决定。

第二十五条 机关、单位对是否属于国家秘密或者属于何种密级不明确或者有争议的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门按照国家保密规定确定。

第三章 保密制度

第二十六条 国家秘密载体的制作、收发、传递、使用、复制、保存、维修和销毁，应当符合国家保密规定。

绝密级国家秘密载体应当在符合国家保密标准的设施、设备中保存，并指定专人管理；未经原定密机关、单位或者其上级机关批准，不得复制和摘抄；收发、传递和外出携带，应当指定人员负责，并采取必要的安全措施。

第二十七条 属于国家秘密的设备、产品的研制、生产、运输、使用、保存、维修和销毁，应当符合国家保密规定。

第二十八条 机关、单位应当加强对国家秘密载体的管理，任何组织和个人不得有下列行为：

（一）非法获取、持有国家秘密载体；

（二）买卖、转送或者私自销毁国家秘密载体；

（三）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体；

（四）寄递、托运国家秘密载体出境；

（五）未经有关主管部门批准，携带、传递国家秘密载体出境；

（六）其他违反国家秘密载体保密规定的行为。

第二十九条 禁止非法复制、记录、存储国家秘密。

禁止未按照国家保密规定和标准采取有效保密措施，在互联网及其他公共信息网络或者有线和无线通信中传递国家秘密。

禁止在私人交往和通信中涉及国家秘密。

第三十条 存储、处理国家秘密的计算机信息系统（以下简称涉密信息系统）按照涉密程度实行分级保护。

涉密信息系统应当按照国家保密规定和标准规划、建设、运行、维护，并配备保密设施、设备。保密设施、设备应当与涉密信息系统同步规划、同步建设、同步运行。

涉密信息系统应当按照规定，经检查合格后，方可投入使用，并定期开展风险评估。

第三十一条 机关、单位应当加强对信息系统、信息设备的保密管理，建设保密自监管设施，及时发现并处置安全保密风险隐患。任何组织和个人不得有下列行为：

（一）未按照国家保密规定和标准采取有效保密措施，将涉密信息系统、涉密信息设备接入互联网及其他公共信息网络；

（二）未按照国家保密规定和标准采取有效保密措施，在涉密信息系统、涉密信息设备与互联网及其他公共信息网络之间进行信息交换；

（三）使用非涉密信息系统、非涉密信息设备存储或者处理国家秘密；

（四）擅自卸载、修改涉密信息系统的安全技术程序、管理程序；

（五）将未经安全技术处理的退出使用的涉密信息设备赠送、出售、丢弃或者改作其他用途；

（六）其他违反信息系统、信息设备保密规定的行为。

第三十二条 用于保护国家秘密的安全保密产品和保密技术装备应当符合国家保密规定和标准。

国家建立安全保密产品和保密技术装备抽检、复检制度，由国家保密行政管理部门设立或者授权的机构进行检测。

第三十三条 报刊、图书、音像制品、电子出版物的编辑、出版、印制、发行，广播节目、电视节目、电影的制作和播放，网络信息的制作、复制、发布、传播，应当遵守国家保密规定。

第三十四条 网络运营者应当加强对其用户发布的信息的管理，配合监察机关、保密行政管理部门、公安机关、国家安全机关对涉嫌泄露国家秘密案件进行调查处理；发现利用互联网及其他公共信息网络发布的信息涉嫌泄露国家秘密的，应当立即停止传输该信息，保存有关记录，向保密行政管理部门或者公安机关、国家安全机关报告；应当根据保密行政管理部门或者公安机关、国家安全机关的要求，删除涉及泄露国家秘密的信息，并对有关设备进行技术处理。

第三十五条 机关、单位应当依法对拟公开的信息进行保密审查，遵守国家保密规定。

第三十六条 开展涉及国家秘密的数据处理活动及其安全监管应当符合国家保密规定。

国家保密行政管理部门和省、自治区、直辖市保

密行政管理部门会同有关主管部门建立安全保密防控机制，采取安全保密防控措施，防范数据汇聚、关联引发的泄密风险。

机关、单位应当对汇聚、关联后属于国家秘密事项的数据依法加强安全管理。

第三十七条 机关、单位向境外或者向境外在中国境内设立的组织、机构提供国家秘密，任用、聘用的境外人员因工作需要知悉国家秘密的，按照国家有关规定办理。

第三十八条 举办会议或者其他活动涉及国家秘密的，主办单位应当采取保密措施，并对参加人员进行保密教育，提出具体保密要求。

第三十九条 机关、单位应当将涉及绝密级或者较多机密级、秘密级国家秘密的机构确定为保密要害部门，将集中制作、存放、保管国家秘密载体的专门场所确定为保密要害部位，按照国家保密规定和标准配备、使用必要的技术防护设施、设备。

第四十条 军事禁区、军事管理区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或者扩大开放范围。

涉密军事设施及其他重要涉密单位周边区域应当按照国家保密规定加强保密管理。

第四十一条 从事涉及国家秘密业务的企业事业单位，应当具备相应的保密管理能力，遵守国家保密规定。

从事国家秘密载体制作、复制、维修、销毁，涉密信息系统集成，武器装备科研生产，或者涉密军事设施建设等涉及国家秘密业务的企业事业单位，应当经过审查批准，取得保密资质。

第四十二条 采购涉及国家秘密的货物、服务的机关、单位，直接涉及国家秘密的工程建设、设计、施工、监理等单位，应当遵守国家保密规定。

机关、单位委托企业事业单位从事涉及国家秘密的业务，应当与其签订保密协议，提出保密要求，采取保密措施。

第四十三条 在涉密岗位工作的人员（以下简称涉密人员），按照涉密程度分为核心涉密人员、重要涉密人员和一般涉密人员，实行分类管理。

任用、聘用涉密人员应当按照国家有关规定进行审查。

涉密人员应当具有良好的政治素质和品行，经过保密教育培训，具备胜任涉密岗位的工作能力和保密知识技能，签订保密承诺书，严格遵守国家保密规定，承担保密责任。

涉密人员的合法权益受法律保护。对因保密原因合法权益受到影响和限制的涉密人员，按照国家有关规定给予相应待遇或者补偿。

第四十四条 机关、单位应当建立健全涉密人员管理制度，明确涉密人员的权利、岗位责任和要求，对涉密人员履行职责情况开展经常性的监督检查。

第四十五条 涉密人员出境应当经有关部门批准，有关机关认为涉密人员出境将对国家安全造成危害或者对国家利益造成重大损失的，不得批准出境。

第四十六条 涉密人员离岗离职应当遵守国家保密规定。机关、单位应当开展保密教育提醒，清退国家秘密载体，实行脱密期管理。涉密人员在脱密期内，不得违反规定就业和出境，不得以任何方式泄露国家秘密；脱密期结束后，应当遵守国家保密规定，对知悉的国家秘密继续履行保密义务。涉密人员严重违反离岗离职及脱密期国家保密规定的，机关、单位应当及时报告同级保密行政管理部门，由保密行政管理部门会同有关部门依法采取处置措施。

第四十七条 国家工作人员或者其他公民发现国家秘密已经泄露或者可能泄露时，应当立即采取补救措施并及时报告有关机关、单位。机关、单位接到报告后，应当立即作出处理，并及时向保密行政管理部门报告。

第四章 监督管理

第四十八条 国家保密行政管理部门依照法律、行政法规的规定，制定保密规章和国家保密标准。

第四十九条 保密行政管理部门依法组织开展保

密宣传教育、保密检查、保密技术防护、保密违法案件调查处理工作，对保密工作进行指导和监督管理。

第五十条 保密行政管理部门发现国家秘密确定、变更或者解除不当的，应当及时通知有关机关、单位予以纠正。

第五十一条 保密行政管理部门依法对机关、单位遵守保密法律法规和相关制度的情况进行检查；涉嫌保密违法的，应当及时调查处理或者组织、督促有关机关、单位调查处理；涉嫌犯罪的，应当依法移送监察机关、司法机关处理。

对严重违反国家保密规定的涉密人员，保密行政管理部门应当建议有关机关、单位将其调离涉密岗位。

有关机关、单位和个人应当配合保密行政管理部门依法履行职责。

第五十二条 保密行政管理部门在保密检查和案件调查处理中，可以依法查阅有关材料、询问人员、记录情况，先行登记保存有关设施、设备、文件资料等；必要时，可以进行保密技术检测。

保密行政管理部门对保密检查和案件调查处理中发现的非法获取、持有的国家秘密载体，应当予以收缴；发现存在泄露国家秘密隐患的，应当要求采取措施，限期整改；对存在泄露国家秘密隐患的设施、设备、场所，应当责令停止使用。

第五十三条 办理涉嫌泄露国家秘密案件的机关，需要对有关事项是否属于国家秘密、属于何种密级进行鉴定的，由国家保密行政管理部门或者省、自治区、直辖市保密行政管理部门鉴定。

第五十四条 机关、单位对违反国家保密规定的人员不依法给予处分的，保密行政管理部门应当建议纠正；对拒不纠正的，提请其上一级机关或者监察机关对该机关、单位负有责任的领导人员和直接责任人员依法予以处理。

第五十五条 设区的市级以上保密行政管理部门建立保密风险评估机制、监测预警制度、应急处置制度，会同有关部门开展信息收集、分析、通报工作。

第五十六条 保密协会等行业组织依照法律、行政法规的规定开展活动，推动行业自律，促进行业健康发展。

第五章 法律责任

第五十七条 违反本法规定，有下列情形之一，根据情节轻重，依法给予处分；有违法所得的，没收违法所得：

（一）非法获取、持有国家秘密载体的；

（二）买卖、转送或者私自销毁国家秘密载体的；

（三）通过普通邮政、快递等无保密措施的渠道传递国家秘密载体的；

（四）寄递、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的；

（五）非法复制、记录、存储国家秘密的；

（六）在私人交往和通信中涉及国家秘密的；

（七）未按照国家保密规定和标准采取有效保密措施，在互联网及其他公共信息网络或者有线和无线通信中传递国家秘密的；

（八）未按照国家保密规定和标准采取有效保密措施，将涉密信息系统、涉密信息设备接入互联网及其他公共信息网络的；

（九）未按照国家保密规定和标准采取有效保密措施，在涉密信息系统、涉密信息设备与互联网及其他公共信息网络之间进行信息交换的；

（十）使用非涉密信息系统、非涉密信息设备存储、处理国家秘密的；

（十一）擅自卸载、修改涉密信息系统的安全技术程序、管理程序的；

（十二）将未经安全技术处理的退出使用的涉密信息设备赠送、出售、丢弃或者改作其他用途的；

（十三）其他违反本法规定的情形。

有前款情形尚不构成犯罪，且不适用处分的人员，由保密行政管理部门督促其所在机关、单位予以处理。

第五十八条 机关、单位违反本法规定，发生重大泄露国家秘密案件的，依法对直接负责的主管人员和其他直接责任人员给予处分。不适用处分的人员，由

保密行政管理部门督促其主管部门予以处理。

机关、单位违反本法规定，对应当定密的事项不定密，对不应当定密的事项定密，或者未履行解密审核责任，造成严重后果的，依法对直接负责的主管人员和其他直接责任人员给予处分。

第五十九条 网络运营者违反本法第三十四条规定的，由公安机关、国家安全机关、电信主管部门、保密行政管理部门按照各自职责分工依法予以处罚。

第六十条 取得保密资质的企业事业单位违反国家保密规定的，由保密行政管理部门责令限期整改，给予警告或者通报批评；有违法所得的，没收违法所得；情节严重的，暂停涉密业务、降低资质等级；情节特别严重的，吊销保密资质。

未取得保密资质的企业事业单位违法从事本法第四十一条第二款规定的涉密业务的，由保密行政管理部门责令停止涉密业务，给予警告或者通报批评；有违法所得的，没收违法所得。

第六十一条 保密行政管理部门的工作人员在履行保密管理职责中滥用职权、玩忽职守、徇私舞弊的，依法给予处分。

第六十二条 违反本法规定，构成犯罪的，依法追究刑事责任。

第六章 附则

第六十三条 中国人民解放军和中国人民武装警察部队开展保密工作的具体规定，由中央军事委员会根据本法制定。

第六十四条 机关、单位对履行职能过程中产生或者获取的不属于国家秘密但泄露后会造成一定不利影响的事项，适用工作秘密管理办法采取必要的保护措施。工作秘密管理办法另行规定。

第六十五条 本法自 2024 年 5 月 1 日起施行。

关于做好 2024 年信息通信业安全生产和运行安全工作的通知

工信厅信管函〔2024〕88 号

各省、自治区、直辖市通信管理局，中国电信集团有限公司、中国移动通信集团有限公司、中国联合网络通信集团有限公司、中国广播电视网络集团有限公司、中国铁塔股份有限公司、中国卫通集团股份有限公司，中国通信企业协会，相关互联网企业，相关通信工程参建单位：

为做好 2024 年信息通信业安全生产和网络运行安全工作，现就有关事项通知如下：

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的二十大和二十届二中全会精神，深入贯彻习近平总书记关于安全生产和应急管理的重要论述，坚持人民至上、生命至上，坚持红线意识、底线思维，坚持高质量发展和高水平安全良性互动，按照安全生产治本攻坚三年行动工作部署要求，把安全生产和网络运行安全的任务、措施、责任真正落到实处，切实筑牢保障人民群众生命财产安全和社会大局稳定的信息通信网络底座。

——坚持安全发展。切实统筹好发展和安全，抓细抓实安全生产和网络运行安全工作，完善安全治理体系，增强安全保障能力，有效防范和坚决遏制重特大事故。

——坚持预防为主。树牢“隐患就是事故”理念，着力消除由于重大风险管控措施缺失或执行不到位而造成的重大事故隐患，推动安全生产治理模式向事前预防转型。

——坚持技管结合。强化科技保障，构建事前风险预警、事中研判处置、事后溯源管理的技术手段体系，增强网络运行智能感知、快速响应、自治自愈能力，提升智能化水平。

二、主要任务

（一）强化思想政治引领。一是加强安全理论学习。深入学习贯彻习近平总书记关于安全生产的重要论述，把理论学习成果转化为谋划工作的创新思路、务实举措和有效方法，把“两个根本”“三管三必须”要求贯穿到安全管理工作全方面各环节。二是树牢安全发展理念。牢固树立全员安全红线意识，把“时时放心不下”的责任感转化为“事事心中有底”的行动力，坚决扛牢防范重大风险的政治责任，坚决克服麻痹思想和侥幸心理，毫不放松抓好安全生产和网络运行各项工作。

（二）完善制度政策体系。一是加强制度体系建设。结合本地区、本单位实际，不断完善安全生产和网络运行安全管理制度，组织做好政策制度宣贯培训，不断提高工作制度化水平。二是加强标准体系建设。制定安全生产和网络运行安全标准化基本规范、5G 网络运行安全风险评估系列标准等，推进安全生产和网络运行安全标准化管理体系建设和评估，持续深入推动

标准落地实施，发挥标准引导规范作用。

（三）增强安全预防能力。一是完善双重预防机制。持续改进安全风险分级管控措施，推广极端事故场景、关键网络设备、高危操作岗位“三项清单”管理，加强事故隐患排查治理。二是增强容灾备份能力。在规划、建设阶段，同步考虑网络运行安全问题，从网元等层面持续加固网络，做好重要设备、链路、业务系统的冗余配置，建立热备或双活机制，提升网络韧性。三是提升云服务可靠性。加强云服务关键节点和重要指标监控，开展云服务倒换测试，检验措施有效性。

（四）加强重点问题整治。一是从严网络操作管理。要严格遵守网络运行重大变更操作管理制度和流程规范，严格权限审批，避免在业务忙时进行风险操作。二是维护配套设施安全。加强对通信机房供电、制冷等配套支撑设施安全风险隐患排查整治，对通信设施“超期限、超负载、超容量”风险隐患开展集中整治。三是严格基本建设流程管理。合理安排建设项目工期，提高工程物料检验、开工前安全技术交底、现场施工人员到岗、竣工验收备案等环节的有效性，加强工程项目中抗震、防雷接地、防火等强制性标准要求在设计、施工和验收等环节的检查落实。

（五）紧盯关键环节场景。一是强化建设环节管理。加强通信建设工程安全生产管理和安管人员的现场履职，重点突出高处作业、带电作业、有限空间作业等危险作业场景管理，特种作业人员应持证上岗，坚决杜绝违章作业，避免发生损害人身安全事故。二是强化运维环节管理。开展网络运行安全管理年活动，持续完善网络运行维护各类规章制度和操作规程，严防违规操作，提升网络运行维护能力。三是强化环境安全管理。加强通信机房、配电室等重点场所防火防雷防爆、用电安全、个体防护等巡查，综合采用人防、物防、技防等手段，及时发现和消除安全隐患，确保人员安全。

（六）提升应急处置水平。一是完善应急预案体系。健全网络故障应急预案体系，充分考虑各类极端场景，完善企业应急处置预案库，强化重点岗位、重点部位现场应急处置方案实操性。二是健全快速响应机制。开展网络运行安全场景化、脚本化演练，提高现网倒换和跨区域跨部门跨专业协同处置能力。三是加强科技力量保障。建设通信网络运行极端事故场景试验验证平台，模拟网络运行极端场景，开展测试验证和模拟演练。

（七）严格执法监督考核。一是完善考核评价机制。各企业要制定本单位考核评价规定，将有关工作情况

纳入绩效考评指标。二是加强日常巡查检查。综合运用“四不两直”、明查暗访等方式深入检查，加大约谈、通报力度，时刻保持“打非治违”高压态势。三是严肃事故责任追究。完善事故责任倒查机制，严格执法监督，依法查处属地信息通信业安全生产和网络运行安全违法违规行为；对发生安全生产和网络运行安全事故，造成不良后果的，依规严肃追责问责相关单位和个人。

三、保障措施

（一）加强组织领导。各地通信管理局要加强指挥调度，认真落实地方政府及安全生产监管部门安全生产工作任务，切实做好本地区信息通信业安全生产和网络运行安全工作。各企业要加强对本单位安全生产和网络运行安全的工作部署，加强对子（分）公司的管理，确保各项要求落实到位。

（二）强化法治保障。积极参与推进电信设施保护立法进程，大力支持制定电信网络运行安全考核评价管理、电信网络运行事故调查处理等规章制度，以及通信建设工程安全生产重大事故隐患判定标准，完善重大事故隐患排查治理的责任体系，为不断推动安全生产和网络运行安全工作提供法治保障。

（三）加大投入保障。各企业要加强统筹规划，加大对安全生产和网络运行安全资金、物资、技术、人员的投入保障力度；建立专项资金使用制度，确保通信工程依规全额向施工企业列支安全生产费；建强安全生产和网络运行安全管理团队，推进人才梯队建设，打通人才职业上升渠道。

（四）强化激励引导。各单位要完善正向激励机制，评选优秀成果、典型案例，总结推广经验；将安全生产和网络运行安全绩效与履职评定、职务晋升、奖励惩处挂钩；鼓励通过安全技能培训、举办安全生产知识大赛等活动，持续提升通信建设领域从业人员安全素质，增强企业安全文化。

请各地通信管理局、各基础电信企业集团于 2024 年 12 月 15 日前，将本地区、本企业 2024 年信息通信业安全生产和网络运行安全工作总结报工业和信息化部。工作中的重要情况和重大问题要及时报工业和信息化部。

工业和信息化部办公厅

2024 年 3 月 19 日

中国共产党党员网络行为规定

(2024 年 1 月 14 日中共中央批准 2024 年 1 月 14 日中共中央办公厅发布)

第一章 总则

第一条 为了规范党员网络行为，发挥党员在网络空间作用，根据《中国共产党党员教育管理工作条例》等有关党内法规，制定本规定。

第二条 本规定所称网络行为，是指通过互联网制作、复制、存储、发布、传播文字、图片、音频、视频等信息内容及其相关活动。

第三条 党员实施网络行为，应当深刻领悟“两个确立”的决定性意义，增强“四个意识”、坚定“四个自信”、做到“两个维护”，坚持正确政治方向、舆论导向、价值取向，严守政治纪律和政治规矩，发挥先锋模范作用，走好网上群众路线，营造健康向上、风清气正的网络环境，推动形 成良好网络生态，维护政治安全和意识形态安全，自觉在思 想上政治上行动上同以习近平同志为核心的党中央保持一致。

第四条 各级党组织承担党员网络行为管理工作主体责任，全面落实网络意识形态工作责任制和网络安全工作责任制。各级组织、宣传和网信等部门在各自职责范围内，负责党员网络行为管理工作。

第二章 网络正能量传播

第五条 党员应当积极通过网络，广泛宣传习近平新时代中国特色社会主义思想，宣传党的路线方针政策和党中央重大决策部署，宣传中国特色社会主义制度，宣传党带领人民团结奋斗的重大成就、历史经验和生动实践，宣传中华优秀传统文化、革命文化、社会主义先进文化，弘扬社会主义核心价值观和社会主义荣辱观，大力弘扬主旋律、传播正能量。

第六条 党员应当践行网上群众路线，密切联系群众，及时反映群众的意见和要求，回应社会关切，解疑释惑、析事明理，引导群众形成共识。

第七条 党员应当敢于斗争、善于斗争，对网上各类错误思潮和错误观点敢于亮剑发声，旗帜鲜明批驳谬误。

第八条 鼓励党员通过网络讲好中国特色社会主义的故事、中国共产党的故事、中国人民奋斗圆梦的故事、中华优秀传统文化的故事、中国和平发展的故事，向世界展现真实、立体、全面的中国。

第三章 网络行为管理

第九条 党员网络行为应当严格遵守党规党纪，模范遵守法律法规，自觉坚守原则和底线。

第十条 党员不得通过网络制作、复制、存储、发布、传播含有反对党的基本理论、基本路线、基本方略，违背四项基本原则，违背、歪曲党的改革开放决策，妄议党中央大政方针，破坏党的集中统一，丑化党和国家形象，诋毁、污蔑党和国家领导人、英雄模范，或者歪曲党的历史、中华人民共和国历史、人民军队历史等有严重政治问题的信息，不得组织、参加含有相关内容的网络论坛、群组、直播等活动。

第十一条 党员不得组织、参与和动员不法串联、联署、集会等网上非法组织、非法活动。

第十二条 党员不得通过网络制造、散布、传播政治谣言，不得匿名诬告、有意陷害或者制造其他谣言。

第十三条 党员不得参与网络宗教活动、迷信活动，不得参与或者纵容、支持利用网络宣扬恐怖主义、分裂主义、极端主义，邪教，或者煽动民族仇恨、民族歧视，破坏民族团结。

第十四条 党员不得擅自建立、使用非法定信道浏览、访问、使用境外的网站、应用程序等。

第十五条 党员应当严格遵守党的保密纪律，不得通过网络泄露、扩散党和国家秘密、工作秘密。

第十六条 党员不得通过发布、删除网络信息，以及其他干预信息呈现等手段谋取不正当利益。

第十七条 党员应当培育良好网络习惯，自觉抵制崇洋媚外、炫富斗阔、铺张浪费等不良网络文化，炒作绯闻丑闻、拉踩引战、刷量控评、直播打赏、沉迷网络游戏等不良网络现象。

第十八条 党员干部不得利用职务便利，索取或者非法收受他人有财产价值的网络账号、网络游戏装备、虚拟货币等网络虚拟财物。

第十九条 党员干部不得违反有关规定以职务身份开展网络借贷、直播带货等营利活动。

第二十条 党员干部注册、使用和管理网络公众账号，应当遵守有关规定，履行社会责任，不得损害国家安全、社会公共利益和他人合法权益。

第二十一条 党员发现网上违规违纪违法信息、活动的，应当及时向有关部门和网络平台举报，积极提供线索，协助有关方面处置。

第四章 保障和监督

第二十二条 各级党组织应当开展党员依规依法上网用网的常态化教育，提升党员网络素养与技能，鼓励和支持党员学网上网用网。

第二十三条 各级党组织应当激励党员在网上充分发挥先锋模范作用，对在网络正能量传播和舆论引导中作出突出贡献的党员，按照有关规定给予表彰奖励，作为评先评优、职务职级晋升、职称评聘等参考。

第二十四条 建立健全澄清正名和保护制度，关心爱护为党和人民利益敢于在网上亮剑发声的党员。对在网络正能量传播和舆论引导中敢于斗争、担当尽责而遭受诬告陷害、网络暴力、威胁恐吓的党员，各级党组织应当协调有关部门依法维护其合法权益，依法惩治有关违法犯罪行为。

第二十五条 各级党组织应当加强对党员网络行为的指导，区分党员不同主体，结合网络公众账号和网络行为类型，形成科学合理的制度规范，健全监督管理制度。

第二十六条 各级党组织应当把规范党员网络行为、发挥党员在网络空间作用作为党的建设的重要内容，纳入党建工作责任制，紧密结合中心工作推进落实。

第二十七条 各级党组织应当将党员网络行为纳入民主生活会、组织生活会对照检查和民主评议党员的重要内容，及时总结经验，通报表扬先进，检视差距和不足，引导和规范党员正确实施网络行为。

第二十八条 党员违反本规定的，根据行为性质和情节轻重，依规依纪追究责任；涉嫌违法犯罪的，按照有关法律规定处理。

第五章 附则

第二十九条 军队党员实施网络行为，按照军队有关规定执行。

第三十条 本规定由中共中央组织部、中共中央宣传部、中央网络安全和信息化委员会办公室负责解释。

第三十一条 本规定自发布之日起施行。

网络反不正当竞争暂行规定

（2024 年 5 月 6 日国家市场监督管理总局令第 91 号）

第一章 总则

第一条 为了预防和制止网络不正当竞争行为，维护公平竞争的市场秩序，鼓励创新，保护经营者和消费者的合法权益，促进数字经济规范持续健康发展，根据《中华人民共和国反不正当竞争法》（以下简称反不正当竞争法）、《中华人民共和国电子商务法》（以下简称电子商务法）等法律、行政法规，制定本规定。

第二条 鼓励和支持经营者依法开展经营活动，公平参与市场竞争。经营者通过互联网等信息网络（以下简称网络）从事生产经营活动，应当遵循自愿、平等、公平、诚信的原则，遵守法律法规规章，遵守商业道德。

经营者不得实施网络不正当竞争行为，扰乱市场竞争秩序，影响市场公平交易，损害其他经营者或者消费者的合法权益。

第三条 国家市场监督管理总局负责监督指导全国网络反不正当竞争工作，组织查处全国范围内有重大影响的网络不正当竞争案件。

县级以上地方市场监督管理部门依法对网络不正当竞争行为进行查处。

市场监督管理部门在查处违法行为过程中，应当坚持依法行政，保证严格、规范、公正、文明执法。

第四条 市场监督管理部门应当会同反不正当竞争工作协调机制各成员单位，贯彻落实网络反不正当竞争重大政策措施，研究网络反不正当竞争工作重大问题，联合查处重大案件，协同推进综合治理。

反不正当竞争工作协调机制各成员单位应当按照职责分工，依法加强金融、传媒、电信等行业管理，采取有效措施，预防和制止网络不正当竞争行为。

第五条 国家鼓励、支持和保护一切组织和个人对网络不正当竞争行为进行社会监督。对涉嫌网络不正当竞争行为，任何单位和个人有权依法向市场监督管理部门举报，市场监督管理部门接到举报后应当及时处理。

行业组织应当加强行业自律，引导、规范会员依法合规竞争。

第六条 平台经营者应当加强对平台内竞争行为的规范管理，发现平台内经营者采取不正当竞争方式，违法销售商品、提供服务，或者侵害消费者合法权益的行为，应当及时采取必要的处置措施，保存有关记录，并按规定向平台经营者住所地县级以上市场监督管理部门报告。记录保存时间自作出处置措施之日起计算，不少于三年。

第二章 网络不正当竞争行为

第七条 经营者不得利用网络实施下列混淆行为，引人误以为是他人商品（本规定所称商品包括服务）或者与他人存在特定联系：

（一）擅自使用与他人有一定影响的域名主体部分、网站名称、网页等相同或者近似的标识；

（二）擅自将他人有一定影响的商品名称、企业名称（包括简称、字号等）、社会组织名称（包括简称等）、姓名（包括笔名、艺名、译名等）作为域名主体部分等网络经营活动标识；

（三）擅自使用与他人有一定影响的应用软件、网店、客户端、小程序、公众号、游戏界面等的页面设计、名称、图标、形状等相同或者近似的标识；

（四）擅自使用他人有一定影响的网络代称、网络符号、网络简称等标识；

（五）生产销售足以引人误认为是他人商品或者与他人存在特定联系的商品；

（六）通过提供网络经营场所等便利条件，与其他经营者共同实施混淆行为；

（七）其他利用网络实施的足以引人误认为是他人商品或者与他人存在特定联系的混淆行为。

擅自将他人有一定影响的商业标识设置为搜索关键词，足以引人误认为是他人商品或者与他人存在特定联系的，属于前款规定的混淆行为。

第八条 经营者不得采取下列方式，对商品生产经营主体以及商品性能、功能、质量、来源、曾获荣誉、资格资质等作虚假或者引人误解的商业宣传，欺骗、误导消费者或者相关公众：

（一）通过网站、客户端、小程序、公众号等进行展示、演示、说明、解释、推介或者文字标注；

（二）通过直播、平台推荐、网络文案等方式，实施商业营销活动；

（三）通过热搜、热评、热转、榜单等方式，实施商业营销活动；

（四）其他虚假或者引人误解的商业宣传。

经营者不得帮助其他经营者实施前款虚假或者引人误解的商业宣传行为。

第九条 经营者不得实施下列行为，对商品生产经营主体以及商品销售状况、交易信息、经营数据、用户评价等作虚假或者引人误解的商业宣传，欺骗、误导消费者或者相关公众：

（一）虚假交易、虚假排名；

（二）虚构交易额、成交量、预约量等与经营有关的数据信息；

（三）采用谎称现货、虚构预订、虚假抢购等方式进行营销；

（四）编造用户评价，或者采用误导性展示等方式隐匿差评、将好评前置、差评后置、不显著区分不同商品的评价等；

（五）以返现、红包、卡券等方式利诱用户作出指定好评、点赞、定向投票等互动行为；

（六）虚构收藏量、点击量、关注量、点赞量、阅读量、订阅量、转发量等流量数据；

（七）虚构投票量、收听量、观看量、播放量、票房、收视率等互动数据；

（八）虚构升学率、考试通过率、就业率等教育培训效果；

（九）采用伪造口碑、炮制话题、制造虚假舆论热点、虚构网络就业者收入等方式进行营销；

（十）其他虚假或者引人误解的商业宣传行为。

经营者不得通过组织虚假交易、组织虚假排名等方式，帮助其他经营者实施前款虚假或者引人误解的商业宣传行为。

第十条 经营者不得采用财物或者其他手段，贿赂平台工作人员、对交易有影响的单位或者个人，以谋取交易机会或者在流量、排名、跟帖服务等方面的竞争优势。

前款所称的财物，包括现金、物品、网络虚拟财产以及礼券、基金、股份、债务免除等其他财产权益。

第十一条 经营者不得利用网络编造、传播虚假信息或者误导性信息，实施下列损害或者可能损害竞争对手的商业信誉、商品声誉的行为：

（一）组织、指使他人对竞争对手的商品进行恶意评价；

（二）利用或者组织、指使他人通过网络散布虚假或者误导性信息；

（三）利用网络传播含有虚假或者误导性信息的风

险提示、告客户书、警告函或者举报信等；

（四）其他编造、传播虚假或者误导性信息，损害竞争对手商业信誉、商品声誉的行为。

客户端、小程序、公众号运营者以及提供跟帖评论服务的组织或者个人，不得故意与经营者共同实施前款行为。

本条所称的商业信誉，是指经营者在商业活动中的信用和名誉，包括相关公众对该经营者的资信状况、商业道德、技术水平、经济实力等方面的评价。

本条所称的商品声誉，是指商品在质量、品牌等方面的美誉度和知名度。

第十二条 经营者不得利用互联网、大数据、算法等技术手段，通过影响用户选择或者其他方式，实施流量劫持、干扰、恶意不兼容等行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行。

前款所称的影响用户选择，包括违背用户意愿和选择权、增加操作复杂性、破坏使用连贯性等。

判定是否构成第一款规定的不正当竞争行为，应当充分考虑是否有利于技术创新和行业发展等因素。

第十三条 未经其他经营者同意，经营者不得利用技术手段，实施下列插入链接或者强制进行目标跳转等行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行：

（一）在其他经营者合法提供的网络产品或者服务中，插入跳转链接、嵌入自己或者他人的产品或者服务；

（二）利用关键词联想、设置虚假操作选项等方式，设置指向自身产品或者服务的链接，欺骗或者误导用户点击；

（三）其他插入链接或者强制进行目标跳转的行为。

第十四条 经营者不得利用技术手段，误导、欺骗、强迫用户修改、关闭、卸载其他经营者合法提供的设备、功能或者其他程序等网络产品或者服务。

第十五条 经营者不得利用技术手段，恶意对其他经营者合法提供的网络产品或者服务实施不兼容。

判定经营者是否恶意对其他经营者合法提供的网络产品或者服务实施不兼容，可以综合考虑以下因素：

（一）是否知道或者应当知道不兼容行为会妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行；

（二）不兼容行为是否影响其他经营者合法提供的网络产品或者服务正常运行，是否影响网络生态开放共享；

（三）不兼容行为是否针对特定对象，是否违反公平、合理、无歧视原则；

（四）不兼容行为对消费者、使用该网络产品或者服务的第三方经营者合法权益以及社会公共利益的影响；

（五）不兼容行为是否符合行业惯例、从业规范、自律公约等；

（六）不兼容行为是否导致其他经营者合法提供的网络产品或者服务成本不合理增加；

（七）是否有正当理由。

第十六条 经营者不得利用技术手段，直接、组织或者通过第三方实施以下行为，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行：

（一）故意在短期内与其他经营者发生大规模、高频次交易，或者给予好评等，使其他经营者受到搜索降权、降低信用等级、商品下架、断开链接、停止服务等处置；

（二）恶意在短期内批量拍下商品不付款；

（三）恶意批量购买后退货或者拒绝收货等。

第十七条 经营者不得针对特定经营者，拦截、屏蔽其合法提供的信息内容以及页面，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平竞争秩序。拦截、屏蔽非法信息，频繁弹出干扰用户正常使用的信息以及不提供关闭方式的漂浮视窗等除外。

第十八条 经营者不得利用技术手段，通过影响用户选择、限流、屏蔽、搜索降权、商品下架等方式，干扰其他经营者之间的正常交易，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序。

经营者不得利用技术手段，通过限制交易对象、销售区域或者时间、参与促销推广活动等，影响其他经营者的经营选择，妨碍、破坏交易相对方合法提供的网络产品或者服务的正常运行，扰乱市场公平交易秩序。

第十九条 经营者不得利用技术手段，非法获取、使用其他经营者合法持有的数据，妨碍、破坏其他经营者合法提供的网络产品或者服务的正常运行，扰乱市场公平竞争秩序。

第二十条 经营者不得利用技术手段，对条件相同的交易相对方不合理地提供不同的交易条件，侵害交易相对方的选择权、公平交易权等，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平交易秩序。

以下情形不属于前款规定的不正当竞争行为：

（一）根据交易相对人实际需求且符合正当的交易习惯和行业惯例，实行不同交易条件；

（二）针对新用户在合理期限内开展的优惠活动；

（三）基于公平、合理、无歧视的规则实施的随机性交易。

第二十一条 经营者不得利用技术手段，通过下列方式，实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为：

（一）违背用户意愿下载、安装、运行应用程序；

（二）无正当理由，对其他经营者合法提供的网络产品或者服务实施拦截、拖延审查、下架，以及其他干扰下载、安装、运行、更新、传播等行为；

（三）对相关设备运行非必需的应用程序不提供卸载功能或者对应用程序卸载设置不合理障碍；

（四）无正当理由，对其他经营者合法提供的网络产品或者服务，实施搜索降权、限制服务内容、调整搜索结果的自然排序等行为；

（五）其他妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为。

第二十二条 经营者不得违反本规定，实施其他网络不正当竞争行为，扰乱市场竞争秩序，影响市场公平交易，损害其他经营者或者消费者合法权益。

第二十三条 具有竞争优势的平台经营者没有正当理由，不得利用技术手段，滥用后台交易数据、流量等信息优势以及管理规则，通过屏蔽第三方经营信息、不正当干扰商品展示顺序等方式，妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，扰乱市场公平竞争秩序。

第二十四条 平台经营者不得利用服务协议、交易规则等手段，对平台内经营者在平台内的交易、交易价格以及与其他经营者的交易等进行不合理限制或者附加不合理条件。主要包括以下情形：

（一）强制平台内经营者签订排他性协议；

（二）对商品的价格、销售对象、销售区域或者销售时间进行不合理的限制；

（三）不合理设定扣取保证金，削减补贴、优惠和流量资源等限制；

（四）利用服务协议、交易规则对平台内经营者的交易进行其他不合理限制或者附加不合理条件。

第二十五条 平台经营者应当在服务协议、交易规则中公平合理确定收费标准，不得违背商业道德、行业惯例，向平台内经营者收取不合理的服务费用。

第二十六条 判定构成妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行，可以综合考虑下列因素：

（一）其他经营者合法提供的网络产品或者服务是否无法正常使用；

（二）其他经营者合法提供的网络产品或者服务是否无法正常下载、安装、更新或者卸载；

（三）其他经营者合法提供的网络产品或者服务成本是否不合理增加；

（四）其他经营者合法提供的网络产品或者服务的用户或者访问量是否不合理减少；

（五）用户合法利益是否遭受损失，或者用户体验和满意度是否下降；

（六）行为频次、持续时间；

（七）行为影响的地域范围、时间范围等；

（八）是否利用其他经营者的网络产品或者服务牟

取不正当利益。

第三章 监督检查

第二十七条 对网络不正当竞争案件的管辖适用《市场监督管理行政处罚程序规定》。

网络不正当竞争行为举报较为集中，或者引发严重后果或者其他不良影响的，可以由实际经营地、违法结果发生地的设区的市级以上地方市场监督管理部门管辖。

第二十八条 市场监督管理部门应当加强对网络不正当竞争行为的监测，发现违法行为的，依法予以查处。

市场监督管理部门在查办网络不正当竞争案件过程中，被调查的经营者、利害关系人及其他有关单位、个人应当如实提供有关资料或者情况，不得伪造、销毁涉案数据以及相关资料，不得妨害市场监督管理部门依法履行职责，不得拒绝、阻碍调查。

第二十九条 市场监督管理部门基于案件办理的需要，可以委托第三方专业机构对与案件相关的电子证据进行取证、固定，对财务数据进行审计。

第三十条 对于新型、疑难案件，市场监督管理部门可以委派专家观察员参与协助调查。专家观察员可以依据自身专业知识、业务技能、实践经验等，对经营者的竞争行为是否有促进创新、提高效率、保护消费者合法权益等正当理由提出建议。

第三十一条 市场监督管理部门及其工作人员、第三方专业机构、专家观察员等对参与调查过程中知悉的商业秘密负有保密义务。

市场监督管理部门的工作人员滥用职权、玩忽职守、徇私舞弊或者泄露调查过程中知悉的商业秘密的，依法给予处分。

第四章 法律责任

第三十二条 平台经营者违反本规定第六条，未按规定保存信息，或者对平台内经营者侵害消费者合法权益行为未采取必要措施的，由市场监督管理部门依照电子商务法第八十条、第八十三条的规定处罚。

第三十三条 经营者违反本规定第七条的，由市场监督管理部门依照反不正当竞争法第十八条的规定处罚。

第三十四条 经营者违反本规定第八条、第九条的，由市场监督管理部门依照反不正当竞争法第二十条的规定处罚。

第三十五条 经营者违反本规定第十条的，由市场监督管理部门依照反不正当竞争法第十九条的规定处罚。

第三十六条 经营者违反本规定第十一条的，由市场监督管理部门依照反不正当竞争法第二十三条的规定处罚。

第三十七条 经营者违反本规定第十二条至第二十三条，妨害、破坏其他经营者合法提供的网络产品或者服务正常运行的，由市场监督管理部门依照反不正当竞争法第二十四条的规定处罚。

第三十八条 平台经营者违反本规定第二十四条、第二十五条的，由市场监督管理部门依照电子商务法第八十二条的规定处罚。

第三十九条 经营者违反本规定第二十八条的，由市场监督管理部门依照反不正当竞争法第二十八条的规定处罚。

第四十条 法律、行政法规对网络不正当竞争行为的查处另有规定的，依照其规定。

经营者利用网络排除、限制竞争，构成垄断行为的，依照《中华人民共和国反垄断法》处理。

第四十一条 经营者违反本规定，有违法所得的，依照《中华人民共和国行政处罚法》第二十八条的规定，除依法应当退赔的外，应当予以没收。

第四十二条 违反本规定涉嫌构成犯罪，依法需要追究刑事责任的，市场监督管理部门应当按照有关规定及时将案件移送公安机关处理。

第五章 附则

第四十三条 本规定自 2024 年 9 月 1 日起施行。

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。

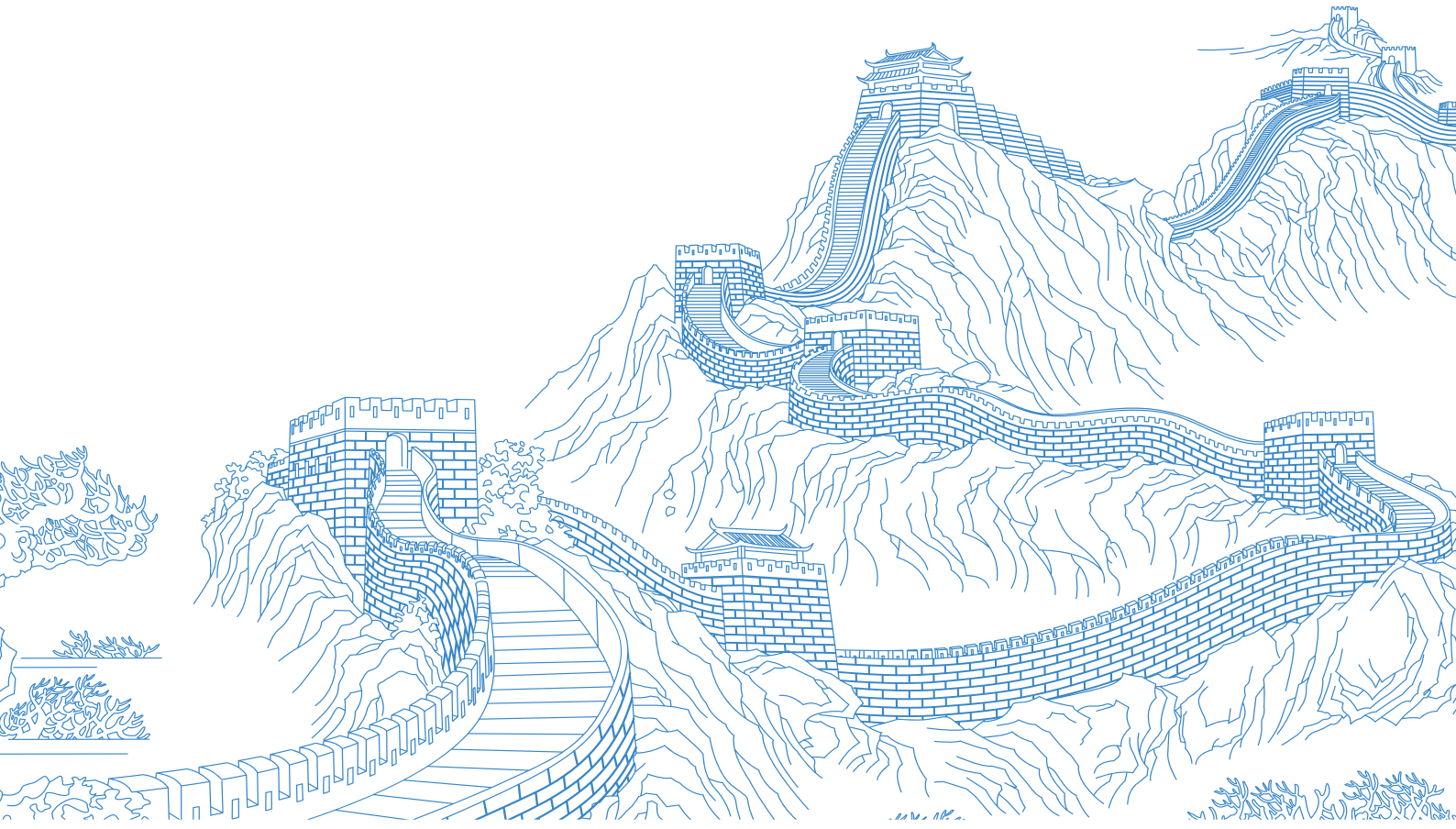
第四十三条 本规定由中央网络安全和信息化委员会办公室、中央机构编制委员会办公室、工业和信息化部、公安部负责解释。

第四十四条 本规定自 2024 年 7 月 1 日起施行。

这十年

我们阔步迈向网络强国

■ 信平



伟大的政党总能够把握时代先机、勇立时代潮头。

十年前的初春，生机萌动、万物竞发。2014 年 2 月 27 日，中央网络安全和信息化领导小组第一次会议在北京召开。在这次重要会议上，习近平总书记首次提出“努力把我国建设成为网络强国”，明确提出了网络强国建设的战略目标，并提出一系列重大论断、作出一系列战略部署，清晰擘画了建设网络强国的宏伟蓝图。这是一个百年大党对时代潮流的引领和把握。纵观世界文明史，人类先后经历了农业革命、工业革命、信息革命。每一次产业技术革命，都给人类生产生活带来巨大而深刻的影响。当信息革命的时代大潮奔涌而来，以习近平同志为核心的党中央统揽全局、把握大势，从人类社会发展的宏阔视角，紧紧抓住信息革命历史机遇，高度重视互联网、大力发展互联网、积极运用互联网、有效治理互联网，走出一条中国特色治网之道。在以习近平同志为核心的党中央坚强领导和习近平总书记关于网络强国的重要思想科学指引下，中国互联网发展迈入了一个全新的历史时期。这十年，中国没有丝毫懈怠、没有丝毫犹豫，奋楫勇进、蹄疾步稳，大踏步赶上并引领时代，网络强国的宏伟图景已清晰可见。

十年回眸看，当惊世界殊。

(一)

马克思指出，蒸汽、电力和自动纺机甚至是“更危险万分的革命家”。他深刻洞察当时先进生产力的巨大影响，天才般地预见了工业革命的世界性冲击。

社会生产力大变革之际，谁能够把握运用这种变革力量，谁就可能把握历史的主动。

1814 年，世界上第一台蒸汽机车在英格兰大地上轰鸣的时候，中国人还不能想象第一次工业革命将成为席卷全球的浪潮，也几乎没有人能够预测，英国会从欧洲一个边陲岛国成为“日不落帝国”。19 世纪，电力的发明和广泛使用，电话、电机以及汽车的出现，意味着以电气革命为标志的第二次工业革命广泛开展，抓住了这波浪潮的美国逐渐成为西方国家的“领头羊”。

顺时代潮流则兴，逆时代潮流则衰。当工业革命发生、世界深刻变革之时，处在封建王朝统治下的中国，没能及时把握世界发展的方向，错失了与世界同步的历史机遇，逐渐落到了被动挨打的境地。特别是鸦片战争之后，中华民族更是陷入积贫积弱、任人宰割的悲惨状况。

错失时代机遇，是每个中国人刻骨铭心的痛。作为 20 世纪人类最伟大的发明之一，互联网给人类社会带来了前所未有的深刻变革，推动人类进入活力迸发、充满希望的信息时代。能不能适应和引领互联网发展，成为决定大国兴衰的一个关键。一定程度上说，得网络者得天下。把握信息革命历史机遇，是事关强国建设、民族复兴的重大战略抉择。

当前，信息革命时代潮流与中华民族伟大复兴战略全局、世界百年未有之大变局发生历史性交汇。习近平总书记深刻指出：“信息化为中华民族带来了千载难逢的机遇。”“我们必须抓住信息化发展的历史机遇，不能有任何迟疑，不能有任何懈怠，不能失之交臂，不能犯历史性错误。”进入新时代，以习近平同志为核心的党中央牢牢把握信息革命的“时”与“势”，统筹推进网络安全和信息化工作。习近平总书记强调“没有网络安全就没有国家安全，没有信息化就没有现代化”，

强调“过不了互联网这一关，就过不了长期执政这一关”，强调“建设网络强国的战略部署要与‘两个一百年’奋斗目标同步推进”，强调“要按照技术要强、内容要强、基础要强、人才要强、国际话语权要强的要求，向着网络基础设施基本普及、自主创新能力显著增强、数字经济全面发展、网络安全保障有力、网络攻防实力均衡的方向不断前进，最终达到技术先进、产业发达、攻防兼备、制网权尽在掌握、网络安全坚不可摧的目标”。

——**技术要强。**“核心技术是国之重器。要下定决心、保持恒心、找准重心，加速推动信息领域核心技术突破”“只有把关键核心技术掌握在自己手中，才能从根本上保障国家经济安全、国防安全和其他安全”。

——**内容要强。**“网络空间是亿万民众共同的精神家园”“坚持正能量是总要求、管得住是硬道理、用得好是真本事”“加强网络内容建设，做强网上正面宣传，培育积极健康、向上向善的网络文化”“形成网上网下同心圆”“健全网络综合治理体系，推动形成良好网络生态”。

——**基础要强。**“我们要加强信息基础设施建设，强化信息资源深度整合，打通经济社会发展的信息‘大动脉’”“要加快构建高速、移动、安全、泛在的新一代信息基础设施，统筹规划政务数据资源和社会数据资源，完善基础信息资源和重要领域信息资源建设，形成万物互联、人机交互、天地一体的网络空间”。

——**人才要强。**“建设网络强国，要把人才资源汇聚起来，建设一支政治强、业务精、作风好的强大队伍”“‘千军易得，一将难求’，要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队”。

——**国际话语权要强。**“要广泛宣介中国主张、中国智慧、中国方案”“加快提升我国对网络空间的国际话语权和规则制定权”“构建网络空间命运共同体，携手创造人类更加美好的未来”。

网络强国战略，吹响了文明悠久的东方大国加速进军信息时代的号角。“五个要强”，旗帜鲜明阐明了中国勇立信息时代潮头的坚定信心，体现了加快发展新质生产力、扎实推进高质量发展的强大决心，体现了把发展主动权牢牢掌握在自己手中的坚强意志。

（二）

1994 年 4 月 20 日，一条 64K 的国际专线从中国科学院计算机网络信息中心接入互联网，实现了与国际互联网的全功能连接，中国成为国际互联网的第七十七个成员。

这一刻，中国互联网时代正式开启，数字浪潮奔涌在中华大地，伟大的中华民族搭上了信息时代的快车，从此，中国发展与互联网更加紧密地结合在一起，也正是通过互联网，中国与世界更加紧密地联系在一起。

从 1994 年到 2014 年的 20 年间，从拨号上网到光纤网络，从每秒 64K 到平均网速突破 3.4M，中国网民规模从零开始到突破 6 亿，数字经济规模达到 16.2 万亿元，一大批网信企业如雨后春笋般涌现而出。

但是，伴随着中国互联网从无到有、从小到大，诸多制约进一步发展的“短板”和“瓶颈”也逐步显现：大而不强、全而不精，自主创新相对落后，关键领域核心技术受制于人，信息化发展程度有待提高，网络安全面临威胁，国际话语权亟须加强……中国已经成为网络大国，但还不是网络强国。

“互联网发展给生产力和生产关系带来的变革是前所未有的，给世界政治经济格局带来的深刻调整是前所未有的，给国家主权和国家安全带来的冲击是前所未有的，给不同文化和价值观念交流交融交锋产生的影响也是前所未有的。”习近平总书记以高度历史自觉和强烈忧患意识，从党的长期执政和国家长远发展的

战略高度，强调必须“使互联网这个最大变量变成事业发展的最大增量”，作出了把我国建设成为网络强国的历史性决策。

风展红旗迈雄关，又踏层峰望眼开。这十年，网络强国宏伟蓝图徐徐展开，网络意识形态主阵地更加巩固，网络综合治理体系建设加快推进，网络安全保障能力全面提升，信息化驱动引领作用充分发挥，网络空间法治化进程不断加快，网络空间国际合作深化拓展，我国正从网络大国向网络强国阔步迈进。

党对网信工作的领导全面加强。坚决贯彻“党管互联网”重大政治原则，全面加强党中央对网信工作的集中统一领导，改革和完善互联网管理领导体制机制，成立中央网络安全和信息化领导小组（后改为委员会），基本建立涵盖中央、省、市的三级网信工作体系，形成“一张网”“一盘棋”的工作格局。

网络空间主流思想舆论巩固壮大。守正创新加强互联网内容建设与管理，大力推动党的创新理论入脑入心，精心做好网上重大主题宣传和重大议题设置，广泛传播社会主义核心价值观，网上正能量更加充沛，主旋律更加高昂。打赢一系列网上重大斗争，根本扭转了过去网上乱象丛生、阵地沦陷、被动挨打的状况，网络意识形态领域形势发生全局性、根本性转变。

网络综合治理体系基本建成。制定实施《关于加快建立网络综合治理体系的意见》，按期完成网络综合治理体系建设目标，推动实现互联网由“管”到“治”的根本性转变。持续开展“清朗”等系列专项行动，针对人民群众反映强烈的网络乱象问题开展集中整治，网络生态日益向善向好。加强网络文明建设，深入实施争做中国好网民工程、网络公益工程，共同培植网上美好精神家园。

网络安全保障体系和能力持续提升。初步建立涵盖网络、系统、终端、应用的网络安全防护体系，强化关键信息基础设施安全保护，加强数据安全管理和个人信息保护，网络安全审查有序开展，网络安全学科和人才建设深入推进。连续十年成功举办国家网络安全宣传周，全社会网络安全防护意识和技能明显提高。

信息化驱动引领作用有效发挥。建成了全球规模最大、技术领先、性能优越的信息基础设施。数字经济蓬勃发展，规模从 2014 年的 16.2 万亿元增长到 2022 年的 50.2 万亿元，总量稳居世界第二。信息领域核心技术产业体系快速发展，实现 3G 突破、4G 同步、5G 引领的重大跨越，北斗卫星导航系统完成全球组网。

网络空间法治化进程深入推进。推动出台《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》《关键信息基础设施安全保护条例》《网络信息内容生态治理规定》等涉网络领域立法 150 余部。持续加大网络执法力度，坚决查处各类违法违规案件，着力维护人民群众在网络空间的合法权益。

网络空间国际话语权和影响力明显增强。携手构建网络空间命运共同体理念更加深入人心，一系列掷地有声的实际行动和成果斐然的合作项目稳步推进。创设并连续十年成功举办世界互联网大会乌镇峰会，成立世界互联网大会国际组织，深度参与网络空间国际治理，提出《全球人工智能治理倡议》，凸显大国道义和国际担当。习近平总书记强调：“网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感。”当前，我国形成了世界上规模最大、生机勃勃的数字社会，截至 2023 年 6 月，网民规模达 10.79 亿，互联网普及率达 76.4%。我国现有行政村全面实现“村村通宽带”，截至 2023 年 6 月，农村互联网普及率达 60.5%，较十年前提升 32.4 个百分点。我国 90% 以上的政务服务实现网上可办，电子政务全球排名上升到第四十三位，成为全球增幅最高的国家之一。分享经济、智慧出行、移动支付等互联网新产品新业态竞相涌现，用得上、用得起、用得好的信息服务正在惠及更多百姓。

这十年，在以习近平同志为核心的党中央坚强领导和习近平总书记关于网络强国的重要思想科学指引下，网信事业从夯基垒台到积厚成势，从发展起步到不断壮大，采取一系列战略性举措，推进一系列变革性实践，实现一系列突破性进展，取得一系列标志性成果，网信事业取得历史性成就、发生历史性变革，这正是新时代十年伟大变革的真实写照和生动体现。

（三）

思想的引领，犹如征途中的旗帜、远航中的灯塔。

马克思主义经典作家生活的时代没有互联网，但是，他们对生产力带来的“危险的”革命性变化的论述仍然熠熠生辉，他们提供的立场、观点、方法，时刻启发着信息时代的马克思主义者。

新时代中国共产党人，以鲜活厚重的理论创新、思想创造，书写了信息时代科学社会主义的光辉篇章。

党的十八大以来，习近平总书记举旗定向、领航掌舵，从信息化发展大势和国内国际两个大局出发，提出了一系列具有开创性意义的新理念新思想新战略，鲜明提出“五个明确”“十个坚持”，系统回答了为什么要建设网络强国、怎样建设网络强国的一系列重大理论和实践问题，明确了事关网信事业发展的一系列方向性、根本性、全局性、战略性重大问题，形成了内涵丰富、科学系统的习近平总书记关于网络强国的重要思想。

引领时代、勇立潮头，紧紧抓住信息化发展给中华民族带来的宝贵历史机遇——

马克思认为，任何真正的哲学都是自己时代的精神上的精华。科学社会主义，自诞生以来就是在解决重大问题中不断丰富发展，保持着蓬勃生机。当今世界，信息革命时代潮流奔涌向前，以互联网为代表的

网络信息技术日益成为创新驱动发展的先导力量，推动社会生产力发生了新的质的飞跃，提出了一系列全新的重大时代课题。习近平总书记以马克思主义政治家、思想家、战略家的非凡理论勇气、卓越政治智慧、强烈使命担当，科学运用马克思主义立场观点方法，立足时代之基，深刻指出互联网是我们这个时代最具发展活力的领域，网信事业代表着新的生产力和新的发展方向，信息化为中华民族带来了千载难逢的机遇。回答时代之问，鲜明提出“谁掌握了互联网，谁就把握住了时代主动权；谁轻视互联网，谁就会被时代所抛弃”。引领时代之变，始终从把握信息时代潮流的高度，对因时而变做好网络安全和信息化工作进行了深刻阐述，彰显出强烈的历史主动精神。

植根实践、引领变革，成功探索走出一条中国特色治网之道——

习近平总书记关于网络强国的重要思想，是在信息时代气象万千的发展变革中逐渐孕育、萌发的，是在中华大地波澜壮阔的生动实践中不断丰富、成熟的，是习近平总书记在党的十八大后领导和推进网络安全和信息化工作实践中发展、形成的。

早在 20 世纪 80 年代，时任河北省正定县委书记的习近平同志就在思索信息时代给中国带来的历史机遇，指出：“科技是关键，信息是灵魂。”世纪之交，在福建，习近平同志极具前瞻性和创造性地作出了建设“数字福建”的重要决策。2003 年，在浙江，习近平同志部署建设“数字浙江”，打造了“百亿信息化建设”工程。2007 年，在上海，习近平同志对不断提高城市信息化水平等作出重要指示要求。

党的十八大以来，以习近平同志为核心的党中央主动顺应信息革命发展潮流，高度重视、统筹推进网络安全和信息化工作。习近平总书记举旗定向、领航掌舵，亲自谋划、亲自部署、亲自推进，推动网信事业发展取得历史性成就、发生历史性变革，成功探索走出一条中国特色治网之道。

习近平总书记关于网络强国的重要思想，深深植根于我国网络强国建设实践沃土，源于实践、指导实践、又被实践所验证，在网络强国建设进程中，展现出坚实的实践基础、鲜明的实践导向和强大的实践伟力。

把握规律、守正创新，为信息时代丰富和发展马克思主义作出了原创性贡献——

创新是互联网的基本属性，是网信事业发展的动力源泉。面对网信领域的一系列前所未有的重大课题，习近平总书记关于网络强国的重要思想，科学回答了马克思主义经典作家没有讲过、前人没有遇到过、西方有关理论无法解决的许多重大理论和实践问题，实现了理论和实践上的重大突破、重大创新、重大发展。

2018 年 4 月 20 日至 21 日，全国网络安全和信息化工作会议在北京召开。习近平总书记发表重要讲话，深刻总结网络强国建设理论创新成果，系统阐述“五个明确”：明确网信工作在党和国家事业全局中的重要地位，明确网络强国建设的战略目标，明确网络强国建设的原则要求，明确互联网发展治理的国际主张，明确做好网信工作的基本方法。

2023 年 7 月，习近平总书记对网络安全和信息化工作作出重要指示，明确提出网信工作“十个坚持”重要原则：坚持党管互联网，坚持网信为民，坚持走中国特色治网之道，坚持统筹发展和安全，坚持正能量是总要求、管得住是硬道理、用得好是真本事，坚持筑牢国家网络安全屏障，坚持发挥信息化驱动引领作用，坚持依法管网、依法办网、依法上网，坚持推动构建网络空间命运共同体，坚持建设忠诚干净担当的网信工作队伍，大力推动网信事业高质量发展，以网络强国建设新成效为全面建设社会主义现代化国家、全面推进中华民族伟大复兴作出新贡献。

这一重要思想，系统运用马克思主义基本原理，结合中华优秀传统文化，以全新的视野对信息时代条件下共产党执政规律、社会主义建设规律、人类社会发展规律进行了深入探索并作出科学回答，为信息时代丰富和发展马克思主义作出了原创性贡献，使科学社会主义在 21 世纪的中国焕发出新的蓬勃生机。

践行宗旨、服务人民，让亿万人民群众共享互联网发展成果——

当前，互联网已经融入社会生产生活的方方面面，越来越成为人们学习、工作、生活的新空间。网信工作与 10 亿多网民直接相连，与 14 亿多人民的获得感、幸福感、安全感息息相关。

习近平总书记站在党的性质宗旨的高度，深刻把握互联网通达亿万群众、连接党心民心的显著特点，多次指出“网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点，让人民群众在信息化发展中有更多获得感、幸福感、安全感”“要适应人民期待和需求，加快信息化服务普及，降低应用成本，为老百姓提供用得上、用得起、用得好的信息服务”“推进‘互联网 + 教育’、‘互联网 + 医疗’、‘互联网 + 文化’等，让百姓少跑腿、数据多跑路，不断提升公共服务均等化、普惠化、便捷化水平”“要走好网上群众路线，提高通过互联网组织群众、宣传群众、引导群众、服务群众的本领，让互联网成为我们同群众交流沟通的新平台，成为了解群众、贴近群众、为群众排忧解难的新途径，成为发扬人民民主、接受人民监督的新渠道”，等等。

习近平总书记的重要论述，深刻回答了网信事业发展“为了谁”“依靠谁”这一根本问题，充分体现了党性与人民性的高度统一、对党负责与对人民负责的高度统一、尊重网信发展规律与尊重人民历史主体地位的高度统一，为网络强国建设注入了最深沉最持久的动力源泉。

胸怀天下、造福世界，为全球互联网发展治理贡献了中国智慧和中国方案——

互联网是人类社会发展的重要成果，真正让世界变成了地球村，让国际社会越来越成为你中有我、我中有你的命运共同体。

随着互联网的快速发展，网络空间发展不平衡、规则不健全、秩序不合理等问题日益凸显，国际社会呼唤新的解决方案。习近平总书记顺应信息时代发展潮流和人类社会发展大势，创造性地提出关于构建网络空间命运共同体的理念主张，深入阐释了全球互联网发展治理一系列重大原则。

这一理念根植于“天下一家”“世界大同”的中国智慧，是人类命运共同体理念在网络空间的具体体现和运用，充满对人类共同命运与人类福祉的深切关怀，彰显了中国共产党为人类谋进步、为世界谋大同的情怀，为全球推进网络空间发展和治理体系变革贡献了中国智慧和中国方案，赢得了世界绝大多数国家特别是广大发展中国家的积极响应和广泛赞誉。

（四）

习近平总书记深刻指出，当今世界，信息化发展很快，不进则退，慢进亦退。

到中流击水，浪遏飞舟。

英国《金融时报》网站刊文指出，“通过与其他国家对比，中国是全球通信、能源和交通领域创新融合发展做得最好的之一，而且中国还有一些独有的特色，使其具备引领这个趋势的能力”。

当前，新一轮科技革命和产业变革向纵深推进，互联网、大数据、云计算、量子信息、人工智能等迅猛发展，既带来了前所未有的机遇，也带来了难以预知的风险挑战和竞争压力。习近平总书记强调，“新时代新征程，网信事业的重要地位作用日益凸显”，要“切实肩负起举旗帜聚民心、防风险保安全、强治理惠民生、增动能促发展、谋合作图共赢的使命任务”“以网络强国建设新成效为全面建设社会主义现代化国家、全面推进中华民族伟大复兴作出新贡献”。

狭路相逢勇者胜。面向新时代新征程，要切实增强信心决心和志气底气，付出更为艰巨、更为艰苦的努力，

奋力实现网络强国战略目标。

实现网络强国战略目标，必须高举思想旗帜。思想是行动的先导。要深入学习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，深刻领会党的创新理论的道理学理哲理，切实将党的创新理论贯彻落实到网络强国建设各方面全过程，推动思想伟力转化为推进网络强国建设的巨大实践动力。

实现网络强国战略目标，必须强化政治担当。“两个确立”是实现网络强国战略目标的最大政治底气，“两个维护”是实现网络强国战略目标的最大政治保证。要加强党对网信工作的全面领导，深刻领悟“两个确立”的决定性意义，增强“四个意识”、坚定“四个自信”、做到“两个维护”，确保网络强国建设始终沿着正确政治方向和道路前进。

实现网络强国战略目标，必须保持战略定力。习近平总书记强调：“对长期任务，要保持战略定力和耐心，坚持一张蓝图绘到底，滴水穿石，久久为功。”当前，网络强国蓝图已经绘就，要咬定青山不放松，以“功成不必在我”的精神境界和“功成必定有我”的历史担当，发扬钉钉子精神，一步一个脚印，扎实推进网络内容建设和管理、网络安全、信息化、网络空间国际交流合作等各项任务，将宏伟蓝图转化为美好现实。

实现网络强国战略目标，必须坚持自立自强。一个民族唯有精神上站得住、站得稳，才能屹立于世界民族之林；唯有不断创新，才能勇立时代潮头、走在发展前列。面对新一轮科技革命和产业变革的历史机遇，要以只争朝夕的紧迫感、逆水行舟的危机感、舍我其谁的使命感，自信自强、守正创新，在新征程上开启网络强国建设的新篇章。

实现网络强国战略目标，必须提升斗争本领。网络强国前进道路上，绝不会一帆风顺，甚至会遇到狂风暴雨、惊涛骇浪。要统筹发展和安全，积极防范化解前进道路上的各种风险，敢于斗争、善于斗争，赢得尊严、赢得主动，切实维护国家主权、安全、发展利益。

实现网络强国战略目标，必须加强开放合作。独行快、众行远。网络强国前进道路上，需要同行人。要秉持开放包容的理念，不断深化网络空间国际合作，会同国际社会共同构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间，构建更加紧密的网络空间命运共同体。

从工业革命时期的落后挨打到信息革命时期的奋力赶超，中华民族的百年历史证明，唯有抓住时代变革的历史机遇，才能实现引领时代的历史跨越。我们深知，信息化与中国式现代化密切相关，网络强国与社会主义现代化强国紧密相连，信息革命时代潮流与民族复兴伟大进程历史交汇，网信事业也处于百年未有之大变局之焦点、引领信息革命时代潮流之先机、关乎中华民族伟大复兴之全局，必须踔厉奋发、勇毅前行，自觉肩负起新时代新征程网信工作的使命任务。

大道无垠，征途壮阔。在以习近平同志为核心的党中央坚强领导下，以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为科学指引，我们必将以更加昂扬的姿态、更加坚定的步伐，向着网络强国战略目标阔步前进，在全面推进强国建设、民族复兴伟业的伟大征程上书写新的壮美篇章。

来源：2024年3月19日
《人民日报》发表署名为“信平”的长篇评论

推动网络安全教育 护航网络强国建设

■ 武汉大学信息中心 曹越
■ 武汉大学国家网络安全学院 李昕煜

随着数字化与信息化技术的不断发展和普及，网络已经深入日常生活中的方方面面，已是现代社会不可或缺的重要组成部分。然而，网络空间正面临着越来越多的威胁和攻击，除个人和非国家组织，此类威胁还涉及到国家之间的网络战争和网络间谍活动。网络空间安全不仅是国家安全的重要组成部分，同时也是构建网络强国的重要支撑和保障。因此，网络强国建设是推动我国高质量发展的重要引擎，两者之间互为表里，相辅相成，确保国家在网络时代的长期繁荣和稳定。

2014 年中央网络安全和信息化领导小组第一次会议上，习近平总书记提出“努力把我国建设成为网络强国”的目标愿景，指出“没有网络安全就没有国家安全”。2024 年是习近平总书记提出网络强国战略目标 10 周年，是我国全功能接入国际互联网 30 周年，而刚刚过去的 4 月 15 日是第 9 个全民国家安全教育日。值此之际，我们有必要全面回顾网络强国战略背景下网络安全教育的发展要求，以及在网络安全教育助力下网络强国建设的辉煌成就，以期通过全社会的共同努力，持续推动全民国家安全教育发展，共建网络安全防线，为网络强国建设注入更多活力。

一、共筑国家安全坚实防线

在当前信息革命时代，数字化、网络化和智能化趋势正深入各经济社会领域，信息流动和共享的速度空前加快，重新塑造着日常生活和工作方式。与此同时，网络安全问题也日益突出，诸如网络病毒、黑客攻击、个人隐私泄露等问题频频发生，给人们的生活和工作带来了巨大的困扰和风险。网络安全是国家安全的重要基石，而信息化数字化成为驱动引领中国式现代化的关键引擎。面对日益复杂的网络安全形势，需要大力推动网络安全教育，增强公众的安全意识，学习网络安全知识，提高自我保护能力。

一是加强对学校的网络安全教育工作普及。学校是青少年成长成才的重要场所，加强网络安全教育，培养学生正确的网络安全意识和行为习惯至关重要。首先，学校可开设专门的网络安全课程或组织网络安全知识竞赛，使学生系统地学习网络安全的基本概念和防范方法；其次，学校可组织网络安全讲座和活动，邀请行业专家向学生和家长普及网络安全知识，提高警惕性和防范意识；最后，学校应建立健全的网络安全监控机制以及培训教职员工了解常见的网络安全威胁和识别网络欺凌等问题的能力，以及时发现和处理学生遇到的网络安全问题。

二是倡导网络安全教育活动的全民共同参与。网络安全为人民，网络安全靠人民，网络安全事关每个人的利益，需要全社会的共同参与和努力。首先，政府部门可通过举办网络安全宣传活动、发布网络安全知识手册等方式，提高公众对网络安全问题的认知，并鼓励社会各界积极参与网络安全教育工作；其次，企业和社会组织也可通过开展网络安全培训、举办网络安全讲座等活动，帮助员工和社区居民提升网络安全防范能力；最后，民众在日常生活中应注意保护个人隐私信息，提高对网络诈骗和网络攻击的警惕性，积极学习网络安全知识。

三是推进网络空间安全政策法律体系宣传。目前，我国已经确立了以总体国家安全观为引领，以《网络安全法》《数据安全法》、《个人信息保护法》为基石，打

造《关键信息基础设施安全保护条例》、《网络安全审查办法》、《网络数据安全管理条例（征求意见稿）》、《数据出境安全评估办法（征求意见稿）》等具体规定为主体的网络空间安全法律体系。然而，上述相关政策法规仍未能被公众所熟知。因此，需加强网络空间安全政策法治体系的在线宣传，通过电视、广播、互联网等多种媒体平台，向公众普及网络空间安全政策法规的内容和重要性，引导人们正确理解和遵守相关法律法规，增强公众对网络安全法治体系的认识和信心。

惟楚有才，于斯为盛。湖北省网信工作一直走在前列，不仅建立了完善的网络安全保障体系，还向公众积极普及网络安全法律法规的教育，致力于为全省人民提供了更安全、更便捷的网络环境，有效维护了网络空间的安全稳定。在第九个全民国家安全教育日来临之际，为增强全民国家安全意识，维护国家安全，中共武汉市委宣传部、武汉市文化和旅游局、武汉市司法局、武汉市公安局、武汉图书馆、众智图书馆联合开展《中华人民共和国网络安全法》专题普法讲座、“政法先锋在行动”系列活动。活动以线下讲座、线上直播的形式，以“刷脸“支付为切入，将法律知识、诈骗案例等融入到平常生活中，深入浅出地为公众传递国家安全观下的个人信息安全重要性，结合“普法讲座 + 互动体验”的创新性表达方式，全力营造人人知晓、支持参与国家安全的浓厚氛围，增强广大群众的法律意识和防骗意识。

二、新时代背景下的网络强国建设

面对百年未有之大变局，建设网络强国不仅意味着技术的领先和信息的安全，更是国家综合国力的体现和国际竞争力的提升，将为构建人类命运共同体提供充沛的数字化动力。网络强国不仅是我国走向现代化的重要标志，也是发展中国式现代化的应有之义。网络安全教育是推动构建网络强国建设的重要保障，近年来，随着网络安全教育的推广，网络空间成为国家发展的重要战略领域，我国网络强国建设不断践行突破。

一是构建泛在智联的数字基础设施服务。网络强国建设离不开数字基础设施，数字基础设施成为全球各国网络空间建设的战略焦点。美国提出万亿级“重建更美好未来”数字基础设施计划，欧盟委员会发布《2030 数字罗盘：欧盟数字十年战略》加速数字基础设施服务建设。我国经建立了全球领先的数字基础设施网络，根据中国信通院测算，预计 2025 年我国 5G 网络建设累计投资将达到 1.2 万亿元，工业企业开展网络化改造投资规模有望达到 5000 亿元。数字基础设施服务体系

4 月 13 日《中华人民共和国网络安全法》专题普法讲座活动在武汉图书馆举办

的建设与完善，为推动数字经济发展、促进社会数字化转型发挥了重要作用，也为网络强国建设奠定了坚实的基础。

二是创新网络空间安全人才培养体系。习近平总书记多次强调：“建设网络强国，没有一支优秀的人才队伍，没有人才创造力迸发、活力涌流，是难以成功的”。2015 年 6 月，为实施国家安全战略，加快网络空间安全高层次人才培养，国务院学位委员会审议，决定在“工学”门类下增设“网络空间安全”一级学科；2016 年，中央网信办、国家发展改革委、教育部等六部门发布《关于加强网络安全学科建设和人才培养的意见》，指出“支持网络安全人才培养基地建设，探索网络安全人才培养模式”；同年，29 所高校获批网络空间安全一级学科博士学位授权点；2017 年 9 月，中央网信办、教育部公布首批一流网络安全学院建设示范项目的 7 所高校名单，2019 年 9 月公布了第二批 4 所入围高校；目前，国内有 60 余所高校设立网络安全学院，200 余所高校设立网络安全本科专业，每年网络安全专业毕业生超 2 万人。我国网络安全人才培养取得了显著成果，稳步推进以高等院校为主体构建适合我国国情的网络安全人才培养模式，初步形成多层次、多形式的网络空间安全人才培养体系。

三是深入推进符合新时代特征的网络强国建设。在网络价值观方面，通过全民国家安全教育日、国家网络安全宣传周、以及“清朗”行动等一列卓有成效的网络强国建设举措，提高了全社会的网络空间安全意识，营造了健康文明的网络环境，正能量氛围在网络空间得到弘扬；在数字资源方面，中央网络安全和信息化委员会发布《“十四五”国家信息化规划》提出建立高效利用的数据要素资源体系，国家数据局等 17 部门联合印发《“数据要素×”三年行动计划（2024—2026 年）》，充分释放数字信息时代的数据要素价值，助力网络强国建设。

结尾

在构建网络空间命运共同体，建设网络强国的伟大征程中，通过广泛开展网络安全宣传教育，提升全民网络安全意识和知识水平，能够共同构筑起坚实的网络防线，守护网络空间的安全与稳定。网络安全教育不仅是保障个人信息安全的必然要求，更是构建网络强国的重要支柱。我们有理由相信，在习近平总书记关于网络强国重要思想的指引下，可以走出一条中国特色网络强国道路。

“国家安全·青春挺膺”主题示范团日活动

4月12日上午，由市两新团工委联合市国安局团委、市互联网行业团委举办的“国家安全·青春挺膺”主题示范团日活动暨互联网行业团委青春走读班在武汉革命博物馆“安邦基石——武汉国家安全教育展”顺利举行，武汉市网络安全协会党支部率部分党员及团员参与本次活动。

“安邦基石——武汉国家安全教育展”通过对总体国家安全观、国家安全法律法规和武汉地区隐蔽斗争史的系统展示，全方位展现了在维护国家安全斗争中的正面典型和反面教材，增强青年国家安全意识，弘扬革命传统。

此次活动旨在加强党员及团员们的国家安全意识，深入了解国家安全的重要性。在活动中，大家仔细参观了展览的各个板块，通过丰富的展品、详细的资料和生动的展示，全面了解了国家安全的各个方面，包括政治安全、军事安全、社会安全、国土安全、经济安全、文化安全等。

参观过程中，党员及团员们认真聆听讲解员的介绍，不时驻足观看，深刻领会了维护国家安全的重要性和紧迫性。大家纷纷表示，网络安全是国家安全的重要组成部分，没有网络安全就没有国家安全，就没有经济社会稳定运行。通过这次参观，对国家安全有了更深刻的认识和理解，将进一步增强责任感和使命感，为维护国家安全做出自己的贡献。

凝心聚力　共筑网安

——武汉联通与武网安协联合开展主题党日活动

为深入学习宣传贯彻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，加强对互联网企业党员的思想引领，促进企业健康发展。为建立健全以学铸魂、以学增智、以学正风、以学促干的长效机制，认真用好党支部主题党日载体，引导党员紧密联系岗位职责和工作要求，深入学习习近平总书记重要讲话和重要指示批示精神。4 月 26 日，武汉联通产业互联网运营中心党支部、武汉联通云网运营中心党支部、武汉市网络安全协会党支部联合开展“以总体国家安全观为指导 全面推进网络强国建设”为主题的党日活动。

会前，党员们共同参观了武汉联通武汉未来城数据中心展示厅。该数据中心是中国联通在中南地区规模最大、功能最全的通信枢纽和信息中心，作为与网络、云计算融合发展的新型基础设施，是各领域各行业信息系统运行的物理载体，汇聚多元数据资源、运用绿色低碳技术、具备安全可靠能力，促进医疗、交通物流、工业互联网、智能制造、云计算等新兴产业集聚成势，赋能千行百业。

随后，全体党员集体观看学习由中央网信办网络社会工作局指导推出的“阔步迈向网络强国”互联网企业微党课系列短视频。北京邮电大学网络空间安全学院党委书记、教授谢永江，针对“推动网信事业行稳致远”等话题，通过视频方式向与会党员进行了一场空中的交流，他深入浅出的阐明了企业党建引领方向，如何将政治优势转化为发展优势，将党建融入管理，将党的建设融入公司治理各个环节，将党建凝聚人心，发挥好服务人民的重要责任，党建激发活力，不断创新

党建工作方式方法，与会党员针对视频内容踊跃讨论发表心得。

交流环节，武汉联通产业互联网运营中心钮世元向与会代表分享了支部党建工作经验。产业互联网运营中心党支部持续以党员为先锋，以共建共联活动为载体，充分发挥党建引领作用，围绕“联网通信、算网数智”，沉淀本地前端急需的重点能力。紧贴集团使命任务，着力聚焦组织领导到位、学习机制到位、深入基层到位、共建共联到位，基于全面打造“既精又专”创新支撑队伍，进一步强化从单一的技术支撑职能部门向市场化主体转型升级，能力建设和市场拓展双轮驱动，以实际行动推动主题教育走心走深走实，助力网安事业高质量发展。

武汉联通产业互联网运营中心华权向与会者介绍了联通数科创新业务能力。据了解，联通数科是中国联通的全资子公司，在原联通系统集成限公司、联通云数据有限公司、联通大数据有限公司、联通物联网有限责任公司、联通智安全科技有限公司基础上组建而成。联通数科在数字化转型领域具有“云网融合、数智领先、安全可信、贴身服务”的优势，集中打造了“云大物智链安”六大创新基础平台能力。

活动交流中，协会党支部书记、秘书长刘悦恒，对本次开展的联合党建活动得到了副会长单位武汉联通的大力支持表示感谢，并介绍协会支部近年来相关工






作情况和成果。本期协会轮值会长（神州绿盟武汉科技有限公司湖北代表处首席代表）陈希艺代表协会感谢会员单位党员积极参与协会组织的党建活动，希望各成员单位今后发挥各自资源优势积极共同谋划形式更加丰富促进共同发展的活动。他还介绍了绿盟科技在武汉近年来的工作重点。

武汉联通产业互联网运营中心党支部书记王晓燕对武汉市网络安全协会党支部及会员单位党员代表一行的到来表示热烈欢迎。她介绍，联通数科通过体系化培养和市场化引进，打造了一支具有高战斗力的专业化、年轻化人才队伍，可提供数字化转型的全面服务。她希望通过本次活动能和各单位多学习、多沟通、多交流，也希望协会发挥桥梁作用，走进其他兄弟企业，更深入地了解企业的需求，更有效地为企业提供帮助。

武汉联通云网运营中心邓晶，就联通自身网络安全建设、人才培养等工作进行了经验分享介绍，欢迎更多专业机构携手同行共同赋能，给予技术支撑和帮助。

智网安云（武汉）信息技术有限公司代表侯志强、杭州迪普科技股份有限公司代表曹钰和曹磊、亚信科技（成都）有限公司代表周冰清、武汉安恒信息科技有限公司代表张博武和邓鹏、湖北天地和兴科技有限公司代表汪立志、武汉达梦数据库股份有限公司代表章莹、协会党支部委员雷侃分别交流发言，共同探讨党建引领与企业发展之路，并希望通过协会平台牵线实现资源共享、优势互补，达成更多合作。

中共武汉市网络安全协会支部成立以来，不断推进社会组织党的组织和党的工作有效覆盖，创新党组织工作内容和活动方式，以党建带会建，以会建促党建，为切实发挥好社会组织党组织的政治核心作用不断探索。

武汉网络安全产业创新大会暨武汉市网络安全协会第二届第二次会员大会成功举办

今年是新中国成立 75 周年，是习近平总书记提出网络强国战略目标 10 周年和我国全功能接入国际互联网 30 周年，为全面贯彻落实习近平总书记关于网络强国的重要思想，推动全市网络安全行业高质量发展，打造网络安全新质生产力，3 月 21 日，在市委网信办指导下，武汉市网络安全协会携手会员伙伴在武汉会议中心共同举办武汉网络安全产业创新大会暨武汉市网络安全协会第二届第二次会员大会

武汉市网络安全协会（以下简称协会）理事长（会长）潘宣辰为大会做工作汇报。回顾去年，协会为加强政治保障正式成立党的组织；为武汉网安发声创办会刊搭建舞台；为规范行业出招启动标准发出倡议；为武汉经济赋能组建智能汽车工委会；为产业创新探索推动网安保险落地；为广结良缘聚势安排多地学习交流；为扩大影响谋划组织各类赛会活动；为人才培养助力编制指南开展培训；为网安宣传加油组织会员投身公益。今年，协会将继续强化党建引领政治保障，促进机构建设规范办会；增强桥梁纽带服务能力，推动产业创新技术进步；围绕我市网信中心工作，提质增效做好各项支撑；建立生态广泛合作，推动实战化人才培养工作；加大投入创新举措，常态化开展网安宣传活动。

本次大会上武汉市网络安全协会正式成立了网络安全保险工作委员会和民办高校工作委员会，并举行了揭牌仪式。

武汉市拥有全国首个国家网络安全人才与创新基地，还拥有全国唯一的国家级科技保险示范区，目前国家正在开展网络安全保险服务试点工作，网络安全保险工作委员会的成立，将加快推动湖北武汉网络安全产业和金融服务融合创新，引导网络安全保险健康有序发展，培育网络安全保险新业态，促进企业加强网络安全风险管理，推动网络安全产业高质量发展作出积极贡献。

武汉作为科教大市，高等教育资源雄厚，其中拥有三十余所民办高校。因民办高校在运营性质与管理模式上具有独特性，在网络安全和信息化建设等方面具有独立性，对网络安全工作的管理也提出了新的要求。成立民办高校工委会，对加强民办高校网络信息化部门的交流协作，推动落实网络安全责任制，探索创新网络安全防御技术，助力数字校园建设，守护教育网络安全，维护师生隐私信息安全，保护科研数据安全，将起到积极推动作用。

2024 年随着数字化转型的加速推进和人工智能技术的快速发展，网络安全将愈发成为各行业关注的焦点。武汉市网络安全协会专家委员会主任、武汉大学国家网络安全学院党委书记赵波教授，为大会带来了《2024 年网络安全技术趋势展望》的主题演讲。赵书记用翔实的数据、生动的事例，全面分析了当前互联网的安全形势，解读了网络空间威胁与挑战、政策导向的基本问题，并对 2024 年网络安全技术趋势进行了展望，针对大家关心的 AI 安全风险问题，赵书记表示，不法分子利用 AI 技术犯罪已经进入一个普及期，未来可能会出现利用人工智能加剧网络犯罪的热潮，AI 带来的安全问题，只能用 AI 来解决。

为切实加强武汉网络安全专家队伍建设，为全市网络安全保障事业，提供集体智慧、展示集体力量、实现集体价值。协会为第四批共计二十位专家颁发了聘书。他们将代表武汉网络安全行业高水平专家智库的集体形象，共同推动武汉网络安全事业高质量发展。

协会智能汽车网络安全专委会成员单位湖北省电子信息产品质量监督检验院软件测评中心副主任李晶

带来了《智能网联汽车网络安全测试现状与解决方案》的专业分享，围绕智能网联汽车网络信息安全安全测评、合规检测、咨询服务等工作提出了一套切实有效的解决方案。

本次大会还特别设置了圆桌讨论环节，武汉市网络安全协会党支部书记、秘书长刘悦恒，武汉大学国家网安学院曹越教授，华中科技大学网络空间安全学院付才教授，岚图汽车数字化发展部总监陶先锋，湖北天融信公司政府事业部总经理吕露分别站在行、校、用、企各自角度共同探讨了武汉网络安全产业创新与人才培养工作，介绍了各自工作经验，提出各自独特看法。

武汉市网络安全协会和武汉市企业信息化促进会联合发布了《信息安全专员能力水平评价规范》团体标准，据介绍，该标准面向企业的信息安全及数据安全从业人员，对其专业知识、工作经验、专业技能等维度构建了一套科学的评价体系。

为选树先进典型，增强“武汉网络安全”集体品牌的凝聚力和影响力，本次大会上协会对 2023 年优秀会

员单位和优秀工作者进行了集体表彰。

本次大会，还收到了来自中国网络空间安全协会、上海信息安全行业协会、昆明市网络安全协会等兄弟协会领导的祝福。同时，大会还举办了网络安全技术创新互动展。

展望未来，武汉网安协会将继续在主管部门的支持指导下，秉承“团结、协作、创新、发展”的理念，不断提升协会的影响力和凝聚力，与各会员、专家伙伴携手同行，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！

省委网信办、国家计算机网络应急技术处理协调中心湖北分中心、市委网信办、武汉网络安全大学筹备专班、市公安局、武汉临空港经开区科经局等行业主管单位相关负责人、二十余所高校网络安全相关专业院系专家教授、一百多家网络安全会员单位代表，共两百多人受邀出席本次活动。

武汉网络安全产业创新大会暨
武汉市网络安全协会第二届第二次会员大会

武汉市网络安全协会 2023 年工作报告

二〇二四年三月二十一日在武汉市网络安全协会第二届理事会第四次会议上

会长　潘宣辰

冬去春来，万物复苏，我们再次相聚一堂，共商网事，共谋发展。我谨代表理事会和秘书处全体职工，向各位会员做协会 2023 年度工作汇报。

2023 年，在主管部门的正确指引下，我们一路披荆斩棘，一路凯歌行进，乘势而上开新局，砥砺奋进谱新篇。坚持围绕我市网信中心工作，支撑主管部门，服务广大会员，做出了各方面积极努力。下面，我从九个方面介绍我会 2023 年的工作，请各位审议：

一、为加强政治保障 正式成立党的组织

根据中共中央办公厅《关于加强社会组织党的建设工作的意见（试行）》和我会《章程》等有关规定，按照主管部门市委网信办、市民政局有关要求，经上级党组织批复，协会于 2023 年 2 月 21 日正式成立了党支部，并顺利召开了协会党支部第一次会议，选举秘书长刘悦恒同志为支部书记。3 月 16 日，武汉市网络安全协会党支部召开了第一次党员生活会暨党支部揭牌仪式。支部全体党员重温入党誓词，向党旗宣誓，全体党员再次接受了心灵的洗礼，决心以更加饱满的热情投身到工作岗位，切实发挥好共产党员的先锋模范作用，努力向党组织交上一份满意的答卷。省委网

信办官方网站对协会党组织的成立予以了关注和转载。

一年来，协会在党支部的带领下，积极发动会员单位，走进安恒、走进汇科智创等单位，联合开展了形式多样的主题党日活动，还走进武昌红巷农讲所组织了“高举党旗跟党走，百年党史寻初心”的党建学习活动。积极发挥协会专业特色，连续承办了多期“党建引领融合赋能”为主题的集聚区专项服务活动，安排党员和专家走进了武汉金融街金融发展集聚区、5.5 医药健康创新园、东湖风景区东湖庭园等，为各类园区机构和群众分析网络安全形势讲解应对技能，得到一致好评。协会支部还在市互联网行业党委的指导下，利用节假日，多次走进全市“江城蜂巢”开展慰问活动，向美好生活的守护者——快递、外卖小哥们送去组织的关心关爱及节日祝福。

协会党组织成立，标志着党建工作迈上了一个新台阶，也标志着我会加快了向规范化专业性社会团体迈进的步伐。协会支部将按照上级党委的工作部署要求，不断完善的党务工作制度，全面加强政治引领和协会党的建设工作，确保协会正确发展方向，树立典型、以点促面，以党组织建设为基础推进协会各项事业健康有序发展。

二、为武汉网安发声 创办会刊搭建舞台

武汉拥有全国首个“国家网络安全人才与创新基地”，目前中央、省、市、区各级主管部门和各方力量不断加大投入，以世界眼光、国际标准、中国特色，搭平台、聚人才、落产业、提能力，大力推进国家网安基地建设，努力打造网络安全人才高地、创新高地、产业高地。但不得不承认，武汉网络安全产业仍然相对弱小，优秀的管理经营、创新产品和技术能力没有集中宣传的媒介，得不到行业内的关注。

为此，协会秘书处精心策划，组建专班投入大量精力资源，创办了《武汉网络安全》通讯会刊，定期向主管部门和会员单位进行赠阅。会刊设立了“政策速递”“党建引领”“武网安人”“协会动态”“各类专栏”等特色栏目，学习网安法规，关注网安产业，发掘网安

人才事迹，宣传武汉网安工作。会刊已经连续发行两期，与协会官网、“武汉网络安全”公众号一起，成为集中展示武汉网络安全产业、技术和人才发展的门户舞台。得到了主管部门和广大会员单位的一致好评。

三、为规范行业出招 启动标准发出倡议

这一年，协会继续加大团体标准规划和编制工作并向行业发布了两项倡议公约。

3 月，我会《中小学信息化设备教学应用净化管理规范》团体标准在第 7 届湖北省教育装备展示交流会上正式发布，本次发布会后，我会秘书长接受了湖北经视专访。本标准起草过程中到了各大媒体的广泛关注，湖北电视台、湖北经视、长江日报、长江网、湖北交通广播等媒体均予以了关注报道。

我会在年中和年底分两批次通过专家评审的方式对《车联网网络安全检测技术要求》《应用系统数据安全能力成熟度模型》《网络安全人才实战化训练环境建设》《数字资产网络安全风险量化评估规范》《数据要素场内流通安全评估技术规范》、《智慧园区网络安全防御体系建设指南》、《制造业数据安全管理中的数据分类分级方法指南》《数据流通隐私保护标准规范》《网络安全服务企业能力技术标准》《信息安全专员能力水平评价规范》十项团体标准予以了立项。目前大部分标准进入编制最后阶段，即将启动征求意见和技术审查工作。争取在 24 年，完成 23 年所有立项标准的发布工作，通过对标准的逐步宣贯，为我市网络安全工作提供规范指引。

为加快构建超大城市网络安全应急指挥管理体系，切实加强和协助主管部门对我市网络安全应急技术支撑队伍的建设和管理工作，我会制定了《武汉市网络安全应急技术支撑单位自律公约》，号召各单位对党忠诚、专业精干、纪律严明、招之能来，来之能战，战之必胜。四十余家单位纷纷响应签署公约承诺。我会还依托智能汽车工委会面向全国发布了全国首个《推动智能汽车网络安全发展倡议书》号召相关产业的企事业单位、高等院校和科研机构，勇于责任担当，托起维护智能汽车网络安全重任、加快科技创新，搭建产学研用交流合作共赢平台、加强行业自律，营造风清气正的行业发展环境。

四、为武汉经济赋能 组建智能汽车工委会

近年来，国家高度重视智能汽车网络安全风险问题，汽车产业是我市经济的支柱产业，我市正依托自身优秀的汽车产业基础大力推动智能网联汽车产业发展。为积极响主管部门号召

4 月，我会在市委网信办的指导下，组织召开了 2023 年武汉市智能汽车网络安全专项工作研讨会，邀请了国家安全中心、东风汽车、武汉大学国家网安学院、华中科技大学网安学院等单位进。深入探讨了智能汽车网络安全与数据安全产业发展现状，分析安全薄弱点和威胁来源，同时基于智能网联汽车市场状况提出了相应建议。随后我会陪同市委网信办相关负责人分赴国家安全中心、武汉经开区、汽车整车制造企业、电子及信息安全领域检验检测机构、网络安全技术企业开展了大量实地调研走访工作。

7 月，在国家计算机网络应急技术处理协调中心湖北分中心、武汉市委网信办的指导下，在国家网络安全人才与创新基地办公室、武汉经开区工委网信办的支持下，武汉市网络安全协会智能汽车网络安全专业委员会正式成立。该专业委员会涵盖了包括东风岚图汽车等整车生产企业、在汉高等院校、检验检测机构、网络安全头部企业等 23 家单位，打通了车路协同各方面资源。

与此同时，工委会面向全国发布了全国首个《推动智能汽车网络安全发展倡议书》、参与支持了在武汉经开区举办的《智能汽车软件大会成功》和《2023 全国智能驾驶测试赛（华中赛区和总决赛）》，启动了《车联网网络安全检测技术要求》团体标准的编制工作，该标准计划与“中国网络空间安全协会”共同发布，并且正积极申请为武汉市地方标准，编制了《交通领域网络安全实战型人才培养指南》、推荐了主任单位岚图汽车荣获网络安全国家标准优秀实践案例一等奖等系列

开创性工作，取得了阶段性成果。

五、为产业创新探索 推动网安保险落地

7月，工业和信息化部 国家金融监督管理总局联合发布了《关于促进网络安全保险规范健康发展的意见》，明确指出：要健全网络安全保险标准规范。支持网络安全产业和保险业加强合作，建立覆盖网络安全保险服务全生命周期的标准体系，研究制定承保前重点行业领域网络安全风险量化评估相关标准，规范安全风险评估要求。

为积极响应国家政策，3月，我会联手众多网络安全科技头部企业和科研机构，武汉东湖科技保险发展促进中心联合人保财险、平安财险、太平洋财险、太平财险、国寿财险、长江财险、中华财险、国任财险等保险机构，签订了战略协议，拟共同联合在网安保险标准规范、平台服务、实验室建设等方面开展深入合作，共建东湖网络安全保险服务中心，为东湖和我市各类型单位提供网络安全金融保障。我会与东湖科保中心组织了多场专题培训和交流活动，各保险公司、网安企业和相关机构踊跃报名参加。

为进一步厘清金融与网络安全相互之间关系，围绕我国数字金融的理论和实践经验，系统考察了数智创新赋能的数字金融创新的内在机制，具体考察了我市数字金融安全存在的隐患、数字化转型中金融安全保障、增强金融领域数据应用安全性与合规性以及网络安全保险落地等问题，我会受市委网信办委托，联合中南财经政法大学金融学院徐晟教授团队开展了《数智创新保障城市数字金融安全》课题研究并顺利结题，取得了阶段性理论成果。

网络安全保险作为风险转移的重要手段可以在转移残余风险、优化资源配置、保障组织财务稳定性和业务连续性等方面发挥重要作用，能够有效聚合各方力量，共同提升网络安全风险治理水平，为此我会将继续加大在此领域的投入，共同为我市数字经济发展和网络强国建设提供重要支撑。

六、为广结良缘聚势 安排多地学习交流

这一年，我会正式代表武汉网络安全产业，加入了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，成为国家级组织正式会员，当选了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。我会秘书处还多次赴北京拜访国家安全中心、中国网络空间安全协会、全国信息安全标准化委员会、国家工业信息安全发展研究中心等国家机构，并参加了中国网络安全产业联盟会员大会，了解了最新国家政策动向并及时传达给我会会员。

为加强兄弟省市网络安全技术交流和产业合作，学习一线城市网络信息安全领域兄弟协会优秀工作经验。我会分赴上海和广州与兄弟协会进行深入交流学习。在上海，上海市信息安全行业协会秘书长王强等协会领导予以热情接待，双方就共同推动网络安全技术创新和产业发展、深化双方合作等方面工作进行了深入探讨，双方一致同意在产业服务、技术创新、人才培养等方面开展深入合作。我会参加了2023北京网络空间安全协会网安联发展工作委员会年会，来自网安联各成员单位的代表、相关领域单位领导、专家、学者以“新时代 新生态 新发展”为话题，共同探讨网安网信事业建设和新时代社会组织高质量发展。我会参与了网民网络安全感满意度调查公益活动，还受邀正式加入公安部三所和北京网安协会主办的《网络与数据安全治理前沿洞察》信息通报机制。

七、为扩大影响谋划 组织各类赛会活动

这一年，我会相继主办、承办参与组织了多项网络安全专业领域赛会活动，进一步提升“武汉网络安全”集体品牌做出了积极努力。

2月底，由武汉市科学技术局、东西湖区经济和信息化局、武汉临空港经开区机电产业建设管理办公室指导，烽火创新谷主办，我会等单位协办的第七届“烽火杯”创新创业大赛总决赛成功举办。通过本次大赛的举办，进一步提高了科技创业者创新创业热情，培养和服务产业链内的中小企业、大学生创业者以及科技

创业者，为他们搭建高层次的交流、学习、合作和资源共享平台，支持创业者发展和企业做大做强。

3 月初，由武汉市人社局、武汉市网络安全协会、武汉安域信息安全技术有限公司联合主办的—2023 年“安域杯”网络安全技能大赛在国家网安基地成功举办大赛聚焦网络安全攻防对抗特色，利用国家网络安全人才与创新基地培训中心优质靶场资源，全方位考察和锻炼选手的攻防实战技能，为我市网络安全产业发掘和培育更多新生人才，共同防御网络威胁，筑牢网络安全防线，保卫国家安全。

3 月底，由武汉市网络安全协会主办，天融信科技集团承办的以“科技赋能共促发展 创新融合共保网安”为主题的金融科技安全发展论坛在武汉举办。论坛聚集了产、学、研、用各方代表近百人出席，共同探讨在金融科技背景下，如何增强金融业务场景下的网络安全防护能力，提升网络安全保障水平，切实有效防范各类风险，促进金融科技迈入高质量发展，积极推动网络安全与金融行业融合创新与发展。

6 月底，由我会主办，理事单位迪普科技承办的 2023 年武汉数据安全创新融合发展峰会成功举办，本次活动邀请到省市区主管部门领导、国家网安基地负责人、有关企业代表共计 300 人参与，峰会以“创新为安 智启未来”为主题，聚焦数据安全技术创新，围绕数据安全基础性战略性前瞻性的技术动向、产业发展趋势和解决方案展开了深入研讨。

8 月，由中国网络安全产业联盟（CCIA）、武汉市委网信办主办“黄鹤杯”网络安全人才创新大赛—创新成果擂台赛暨 2023 年网络安全优秀创新成果大赛武汉分站赛成功举办。武汉分站赛由我会和武汉网络安全技术有限公司共同承办，武汉迪马创聚场科技企业孵化器有限公司、武汉安恒信息科技有限公司协办。武汉分站赛评审专家组由来自武汉高校、科研机构、行业部门的专家与 CCIA 专家委专家、网络安全投资机构专家组成。来自全国 30 余家网络安全企业提交的近 40 项解决方案和创新产品参加了本次比赛。经过评审，武汉分站赛最终评选出“2023 年网络安全优秀创新成果大赛”入围奖 13 项。

9 月 -10 月，我会还积极承办了“黄鹤杯”网络安全人才创新大赛—校园新星赛，大赛分别走进了武汉理工大学、湖北大学、江汉大学、武汉交通职业学院、武汉城市职业学院、武汉职业技术学院等高校，挖掘一批网安新星，持续传递友谊火种。

11 月，我会参与协办了 2023 中国 5G+ 工业互联网大会“数据安全平行会议”，该大会以“筑牢数据安全底座，护航数字经济发展 ”为主题，共同探讨推动数字技术发展与安全的共同促进，为新型工业化高质量发展建言献策。

12 月，我会成功协办了 2023 年湖北省“楚慧杯”网络空间安全实践能力竞赛。本次竞赛以科学合理的赛程设置、实践实战的赛题设计为特色，汇聚全省乃至全国网络安全精英同台竞技，为参赛选手提供了锻炼攻防实战能力、提高专业技能的绝佳学习交流机会。本届竞赛移师国家网安基地，共吸引省内外 403 支战队竞相报名参赛，汇聚了全国上千名网络安全精英，经过预赛激烈的角逐，和决赛精彩的争夺，48 支战队脱颖而出。本次颁奖仪式上，我会正式与华中科技大学、湖北省大数据中心、湖北生物科技职业学院、安恒信息签署了产学研战略合作协议。

这一年，我会受市公安局网安支队推荐，组织了多场网络安全等级保护定级专家评审会，指导协会各会员单位召开了各单位产品技术宣贯活动，如绿盟科技 2023 合作伙伴大会武汉站暨云化产品发布会、盛邦安全 2023 武汉站渠道会等。各项活动精彩纷呈，协会影响力持续扩大。

八、为人才培养助力 编制指南开展培训

为支撑国家网络安全人才与创新基地建设，带动产业上下游产学研合作，我会积极联络工信部人才交流中心，武汉市职业技能鉴定指导中心加强沟通合作。陪同主管部门相继走访江汉大学、华中师范大学等十余所高校，了解全市网络安全人才培养情况。

为深入贯彻落实习近平总书记关于网络强国的重

要思想，加快推进网络安全实战型人才培养，我会受主管部门委托，统筹了八大领域《网络安全实战型人才培养指南》的编制工作，积极协调各编制单位，规范各项工作，推动八项指南课题顺利完成结题任务。

与此同时，我会还承接了 2023 年武汉市网络安全实战型人才“江城卫士”网络安全创新实践班培训工作，邀请了来自北京的学者和行业技术专家亲自授课，通过实训 + 带训 + 实景攻防演练的创新培训模式，让参训学员了解网络安全相关技术发展形势、熟悉法律法规要求、提升网络安全攻防技能、强化综合实战能力，更好的保障我市的网络系统和数据的安全。来自全市关键信息基础设施领域网络和信息安全负责人 200 多人，参与了为期五天的封闭式集训。

培训期间，武汉市网络安全协会志愿者服务队在国家网络安全才人与创新基地成立，团市委学校部副部长岳峥嵘、武汉市网络安全协会政企服务部主任乔奇共同为志愿者服务队授旗。我会成立网络安全志愿服务队，意义重大使命光荣，服务队将恪守“爱网护网，共守清朗”的宗旨，投身到社会服务实践中，维护文明、和谐、清朗的网络空间。

这一年，我会还积极开展面向社会的职业技能认定工作，在武汉市职业技能鉴定指导中心指导下，支持副会长安域公司开展全市首批二级网络信息安全管理员认定考试工作，多位考生顺利通过考核。

九、为网安宣传加油 组织会员投身公益

9 月，协会继续在主管部门的统一部署下，调动广大会员资源，加入到以“共建网络安全 共享网络文明”为主题的 2023 年武汉市国家网络安全宣传周系列活动中去。组织各会员和志愿者参加网络安全进基层工作，配合主管部门拍摄网络安全宣传周长江主题灯光秀，还利用公安反电诈系统、东风智能网联汽车和中国电信 IPTV 电视、手机彩铃等向全市开展沉浸式宣传教育。除此之外，还将围绕“文明上网”“健康上网”“安全用网”等主题，推出海报、手绘、VR、微动漫等系列新媒体作品，用喜闻乐见的方式向市民科普文明上网知识，倡导大家争做文明好网民。我会代表武汉网安产业，参加了湖北省国家网络安全宣传周主会场系列活动，组织会员在黄鹤楼下拍摄公益宣传视频，推荐了理事单位武汉同德兴公司的中小学净屏系统解决方案荣获湖北省国家网安周网络安全优秀实践案例荣誉。

与此同时，作为武汉经开区国家网安周系列重要活动之一，我会在岚图汽车总部成功主办了 2023 年武汉网络安全公益行“智能汽车网络安全大讲堂”活动。活动中，我会与岚图汽车、武汉大学国家网络安全学院、天融信科技集团代表，签约智能汽车网络安全产学研战略合作，将立足智能汽车网络安全，政企校协同合作共同推进产业技术攻关，落实各项网络安全保护措施，切实筑牢汽车企业网络安全屏障。

回首过去，我们无比自豪，展望未来，我们信心百倍。武汉市网络安全协会将继续秉持着‘服务会员、服务行业、服务政府、服务社会’的宗旨，不断加强自身建设，提高服务水平，为推动武汉市网络安全事业的发展做出更新更大的贡献！

武汉市网络安全协会第四批专家名单

韩兰胜

华中科技大学网络空间安全学院教授，博士生导师，武汉市黄鹤英才，武汉市东西湖区政协委员，无党派人士。华科国家网安基地创新与实践中心主任，系统与软件安全研究所教学、科研骨干。长期从事网络、信息安全方面的教学、科研工作，是国家有关部门多项安全项目负责人。主要研究方向为网络安全：恶意代码、移动网络安全、网络行为分析以及大数据安全理论与技术。担任多家国内外期刊网络评审、第二届国际网络安全与可信计算（NSTC2011，Busun Korea）会议执行主席，自 2008 年起担任国家自然科学基金网评，自 2009 年起担任国家大学生信息安全竞赛网评，自 2015 年起担任教育部全国优秀硕士论文网评。2013 年创建华科黑帽子团队、2016 年创建华科网安 CTF 俱乐部、大学生信安大赛创新实践能力赛华中赛区技术委员及负责人。 近年来，主持、协助、参与相关部门对智能终端大数据收集工作，有力维护社会稳定；主持、参与湖北省自科基金、国家自科基金青年及面上项目 5 项，其他项目 10 余个；获得校教学质量优秀奖 1 项、大学生创新创业项目优秀指导教师 3 项、校优秀班主任 3 项、各类网络安全攻防竞赛、护网实测案例等奖项 10 余个。

严飞

武汉大学国家网络安全学院院长助理，教授，博士生导师，湖北省网络空间安全研究中心副主任。中国可信云社区（ChinaSigTC）主要发起人之一。主持和参与了国家自然科学基金、973、863 课题、湖北省重大科技专项以及华为、浪潮、大唐等企业合作多项，完成一款民用可信计算机安全测评系统，完成一款自主可控的可信云系统，主要参与国家安全技术标准制定 2 项，获湖北省科技进步一等奖 2 项、二等奖 1 项。

曹越

武汉大学国家网络安全学院网络空间安全系系主任、教授、博士生导师、湖北珞珈实验室兼职教授。英国计算机学会 - 会士、英国皇家学会工艺院 - 会士、英国高等教育学会 - 会士、IEEE- 高级会员。入选中国高被引学者 (2021-2022，网络空间安全学科，爱思唯尔 & 上海软科发布)、全球前 2% 顶尖科学家“年度影响力”榜单 (2019-2022，爱思唯尔 & 斯坦福大学发布)，湖北省经济和信息化厅“科技副总”(2022)、“武汉英才”产业领军人才 (2021)、国家级 (海外) 青年人才 (2019)。

洪亮

武汉大学信息管理学院大数据安全与保密系书记、副主任、数据科学专业负责人、教授、博士生导师。获得武汉大学人文社科优秀青年学者、武汉大学珞珈青年学者等人才称号；指导学生获得“花旗杯”金融创新应用大赛全国二等奖，荣获“优秀指导教师”称号。获得湖北省自然科学优秀学术论文二等奖，图书情报顶级国际会议 JCDL 2020 最佳实践论文奖，武汉市社会科学优秀成果奖，中国科技情报学会创新团队奖，湖北省自然科学基金创新群体成员等奖励。获邀撰写中国工程院《全球工程前沿 2022》工程管理篇，向全球发布知识大图的研究前沿与热点。多次受邀在北京大学，南京大学等高校，银保监会等政府部门，以及 iConference、JCDL、KDD、教育部金融教指委“金融学术能力提升大讲堂”、知识服务与情报工程学术交流会、《管理世界》大讲堂、CNCC 全国计算机大会等国内外学术会议做报告或担任程序委员会主席、委员等职务。

王虎

武汉理工大学管理学院信息管理与信息管理系专业负责人、教授，博士生导师、企业信息化研究所所长。湖北省“国家中小企业创新基金”专家评委，科学出版社信息管理与信息系统专业本科生系列教材编委会委员，广西工学院特聘教授，国际项目管理协会和项目管理研究委员会认证的项目管理专家。作为核心编委筹划并参与《IT 信息化项目管理知识体系 iPMBOK 与国际项目管理专业资质认证标准》的撰写，主编《管理信息系统》、《电子商务》教材两部。以独撰或以第一作者的身份累计发表学术论文 60 余篇，其中在《科学学与科学技术管理》、《计算机系统应用》、《计算机工程与应用》等权威期刊上发表论文 30 余篇，外文学术杂志和国际学术会议发表论文 (英文) 论文 20 余篇，其中十余篇论文被 SCI/SSCI 收录。

徐晟

中南财经政法大学金融学院教授、博士生导师、金融科技研究院执行院长，研究方向：金融市场、风险管理。湖北省第十一批优秀科技副县（市、区）长；中南财经政法大学优秀硕士生导师。主持过多项部省共建课题及国家社科基金项目；曾获 2018 年获湖北省政府发展研究奖二等奖，2014 年获湖北省省委决策支持工作优秀成果三等奖。2013 年获第八届湖北省社会科学优秀成果奖三等奖；2009 年获湖北省优秀教学成果奖二等奖；

崔新强

原武汉市信息中心网络部部长，1985 年毕业后一直在武汉市信息中心工作，主要承担武汉市电子政务及政务网络建设工作。

龙翔

湖北生物科技职业学院党委委员、副校长，教授，华中科技大学网络空间安全专业博士，省教育厅评选的全省高校优秀“双带头人”党支部书记、湖北省网络安全校企联盟理事长。主持及参与国家自然科学基金项目、工业和信息化部产业发展促进中心重大项目等国家级教研项目 8 项，省级项目 13 项，荣获省级以上教学成果奖 3 次，获得实用新型专利 1 项，软件著作权 4 项。发表论文 11 篇，其中北大核心 2 篇。主编教材 8 本，其中《网络安全协议分析》被评选为职业教育“十四五”国家规划教材。同时，作为专家参与信息安全相关的 1+X 证书的研制工作，深度参与全国职业院校技能大赛、职业院校教师教学能力大赛等技能竞赛活动的评审、执裁工作。

何鹏

湖北大学网络空间安全学院副院长、副教授、湖北省教育信息化工程技术研究中心副主任、智能网联汽车网络安全湖北省工程研究中心副主任、智能感知系统与安全教育部重点实验室骨干成员，全国大学生信息安全大赛特聘专家、湖北省 801 网络空间安全研究院特聘研究员、湖北省网络空间安全学会委员。研究方向包括软件系统的缺陷检测、网络恶意流量分析，区块链与数据安全等。主持国家青年基金项目和省重点研发计划项目，参与国家 973 项目、面上基金项目共 3 项、省部级项目 2 项；在国内外期刊 / 会议上发表论文 50 余篇，获湖北省科技进步奖二等奖 1 项、国家发明专利授权 3 项，软件著作权 12 项。

周伟

华中师范大学信息化办公室网络安全主管、高级工程师、武汉大学信息安全博士。获得 CISSP、CISA、CCSK、ISO/IEC 27001 Foundation、ISO/IEC AUDITOR、CISP、CCAA ISMS 审核员资格，兼任湖北省财政厅评标专家、2022 年度湖北省网络安全等级保护工作专家。在《计算机应用》、《计算机工程与应用》、《小型微型计算机系统》等期刊上发表 20 余篇。获发明专利 2 项，软件著作权 5 项。20 年网络安全从业经验，实践经验丰富，参与多个大型网络安全集成项目建设和运维，为数十家公司提供网络安全管理体系咨询。

张帆

武汉轻工大学数学与计算机学院软件工程系系主任、副教授、硕士生导师、博士。主要从事信息系统安全、软件安全、机器学习及其安全相关研究。主持或参与国家自然科学基金、省杰出青年基金、省自然科学基金等项目 6 项，在 CCF 推荐外文会议和期刊、CCF 推荐中文期刊 A 类等发表论文 20 余篇。授权国家发明专利 6 项。主持或参与省级教学改革项目 3 项。主持省级一流课程 1 项。

孙智

武汉东湖科技保险发展促进中心主任，高级经济师，武汉大学工商管理专业和金融专业硕士研究生导师、中南财经政法大学保险专业硕士，研究生导师、湖北省保险学会智库专家、中国诗歌学会会员、中华诗词学会会员、中国楹联学会会员、中国观赏石协会会员、中国保险书画艺术研究会会员、湖北省作家协会会员、湖北省书法家协会会员、湖北省美术家协会会员、湖北省楹联学会会员。曾是农村知青、军队士兵、商业职工。曾任中国人保财险宜昌市分公司总经理、三峡工程保险研究会会长、中国人保财险湖北省分公司高级专家。

李阳

武汉新时通信息技术有限公司总经理，毕业于华中科技大学计算机系。有在包括用友、上海复华、北京英克、武汉天喻等国内多家知名 IT 上市公司工作经历，且从事网络安全行业工作超过 15 年。作为湖北省信息网络安全协会发起单位之一，历任第一届协会会长，现为武汉网络安协会理事、湖北省信用服务协会秘书长、湖北省财政招投标专家库专家。

袁勇

上海市锦天城（武汉）律师事务所副主任，硕士研究生，第六届武汉市律师协会金融专业委员会副主任和合伙人、湖北省企业管理咨询协会副会长、湖北省法学会警察法学会副秘书长、常任理事、武汉市涉案企业合规第三方监督评估机制专业人员名录库首批人员。主要从事网络监管和行政处罚的外部咨询、数据合规等法律服务。

杨杭杭

武汉地铁桥隧管理有限公司综合部经理、高级工程师、工程硕士，中共党员，研究方向企业管理信息化和信息安全。武汉地铁集团有限公司评标专家库专家，知网 CNKI 评审专家库专家，PMP 国际注册项目管理师，ISO27001 信息安全管理体系认证。主持完成武汉轨道交通多条线路 OA 办公网络和数据中心项目建设和运维，指导完成超级工程武汉长江公铁隧道信息等级保护第三方测评和信息系统安全整改项目建设和实施。独著有《计算机信息安全技术与工程实施研究》专业技术书籍，在国家和省级权威期刊上发表学术论文多篇，授权有《一种计算机网络设备用线材拆分系统及拆分方法》发明专利。获评武汉地铁集团优秀共产党员、突出贡献个人、先进工作者，平安建设先进个人等荣誉称号。

何双江

武汉烽火信息集成技术有限公司，高级工程师、技术总监，计算机专业硕士，湖北省安全可靠电子政务工程技术研究中心主任，湖北大学人工智能校外硕导。在中国信息通信科技集团工作 14 年，深耕 ICT 领域，在人工智能、信创系统、网络安全、政务信息安全等多个领域开展工程和科研实践。曾获得湖北省科技创新团队 (第二)、武汉英才、湖北省科技进步二等奖、武汉市科技进步二等奖、武汉市科技进步三等奖，武汉市双创科技十佳项目。近年申请发明专利 23 项，其中 3 项区块链相关专利获得直接经济价值超过 4096 万。在相关领域发表高水平论文被 SCI/EI 收录 13 篇。承担及参与国家、省、市科技项目 13 项，重大工程项目 15 项。

艾微

中金数据（武汉）超算技术有限公司总经理和中金数谷科技有限公司政企事业部总经理，大学本科，攻读武汉大学 EMBA 硕士，中共党员，研究方向云计算、大数据、IDC、信息系统安全。长期主持中金数据的重大经营及技术决策，对公司科技发展方向、产品结构、服务质量、业务发展等负责并推动实施。获得 7 项国家认证专利及 27 项软件著作权，深耕云技术、大数据、AI、区块链等技术业务 18 年，主导筹备成立烽火通信云计算和数据中心产品线，同年参与筹建湖北省楚天云公司，主导楚天云公司顶层架构的设计、IDC 及云平台的设计实施，直至交付运营，并参与编写《楚天云建设实践》。参与编制《人工智能企业评估标准与评估规范》（T/HBSIA 001-2023），推动湖北省人工智能快速发展，得到武汉市主管部门高度肯定和表扬，被东西湖区委区政府授予网络安全事业创新发展“先进个人”。

杨希彬

武汉网络安全技术有限公司董事、总经理，大学本科，中级经济师，曾在原市政务服务管理办公室公共资源交易管理处、综合处、审批服务协调处从事信息化、人事管理、窗口管理工作，曾任武汉市江汉区科学技术和经济信息化局 党组成员、副局长（挂职）。曾参与组建武汉云科技有限公司、黄鹤网络安全实验室等项目。

石祖文

武汉市有安科技有限公司 CEO，CNNVD 中国国家漏洞库首批特聘专家，知名安全著作《大型互联网企业安全架构》作者。2007 年 7 月参加工作，近 20 年信息安全行业从业经验，早年开发的多款安全工具享誉安全界。参与过政府、奥运、电信和多家世界 500 强集团大型信息安全体系建设，历任 360 Web 安全技术负责人、星云融创首席科学家、挖财首席安全官、华为首席安全专家、以及多家世界 500 强企业安全负责人职位。参加过多个知名安全大会演讲（XDEF、OWASP、WOT 等）。既负责过千人规模员工的互联网金融公司整体安全从零开始的体系建设，也负责过像华为这样拥有十几万雇员的世界级 500 强企业全球化的网络安全与隐私保护体系建设。

何伊圣

山石网科通信技术有限公司资深总监，高级工程师（软考），CCF 计算机安全组委会执行委员、广东省网络空间安全专委会委员。获得 CISP、CISSP、CISA、CCSA、PMP 专业资格证书，首届红帽杯安全企业组冠军、第一届网鼎杯玄武组初赛第一名。

2023 年度优秀会员单位名单

(排名不分先后)

序号	优秀会员单位
1	中国联合网络通信有限公司武汉市分公司
2	武汉安恒信息科技有限公司
3	湖北天融信网络安全技术有限公司
4	湖北星野科技发展有限公司
5	神州绿盟武汉科技有限公司
6	湖北珞格科技发展有限公司
7	武汉观安信息技术有限公司
8	杭州迪普科技股份有限公司
9	湖北中网科技有限公司
10	智网安云（武汉）信息技术有限公司
11	上海三零卫士信息安全有限公司
12	恒安嘉新（北京）科技股份公司
13	武汉市德发电子信息有限责任公司

序号	优秀会员单位
14	亚信科技（成都）有限公司
15	湖北东方网盾信息安全技术有限公司
16	武汉思普崚技术有限公司
17	武汉艾迪时代网络技术有限公司
18	深圳市魔方安全科技有限公司
19	武汉安域信息安全技术有限公司
20	武汉同德兴信息技术有限公司
21	泰和泰（武汉）律师事务所
22	曙光网络科技有限公司
23	蓝芽网络技术（湖北）有限公司
24	湖北天地和兴科技有限公司
25	武汉汇科智创科技有限公司
26	武汉大数据产业发展有限公司

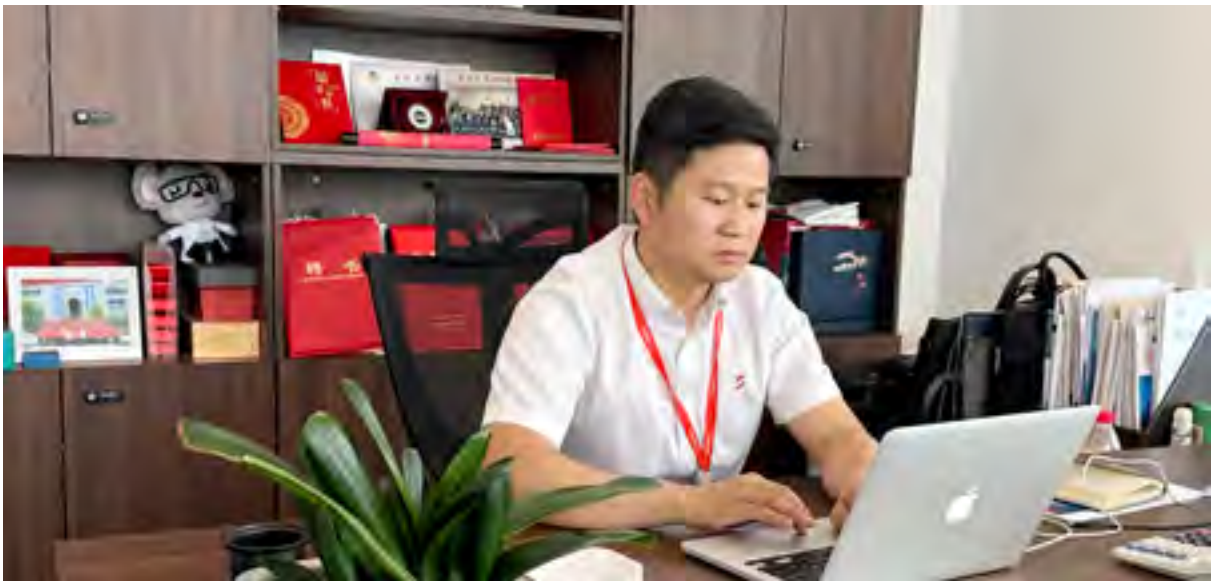
2023 年度优秀工作者名单

（排名不分先后）

序号	姓名	优秀工作者
1	彭建军	武汉安恒信息科技有限公司
2	李　荣	湖北东方网盾信息安全技术有限公司
3	王志豪	中国联合网络通信有限公司武汉市分公司
4	汪天武	杭州迪普科技股份有限公司
5	雷彦章	曙光网络科技有限公司
6	吴成鹭	武汉艾迪时代网络技术有限公司
7	李　航	蓝芽网络技术（湖北）有限公司
8	方　浩	湖北中网科技有限公司
9	刘培培	武汉同德兴信息技术有限公司
10	蔡松强	亚信科技（成都）有限公司
11	向仕华	武汉汇科智创科技有限公司

序号	姓名	优秀工作者
12	周阳波	智网安云（武汉）信息技术有限公司
13	汪立志	湖北天地和兴科技有限公司
14	邓亚洲	神州绿盟武汉科技有限公司
15	黄国忠	深圳市魔方安全科技有限公司
16	杨柳林	泰和泰（武汉）律师事务所
17	管鹏飞	湖北珞格科技发展有限公司
18	李　玲	武汉安域信息安全技术有限公司
19	李　勇	武汉市德发电子信息有限责任公司
20	刘　琼	武汉思普崚技术有限公司
21	朱雪冰	武汉观安信息技术有限公司
22	张　映	湖北天融信网络安全技术有限公司

优秀工作者｜彭建军
——华中网络安全守卫者



今天要为大家介绍的是武汉安恒信息科技有限公司总经理彭建军的先进事迹。党的二十大报告指出，“推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定。必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿党和国家工作各方面全过程，确保国家安全和社会稳定。如今，我们工作、生活的方方面面都离不开网络，如何保障网络、信息安全，守护群众、国家利益，成为了他的使命。

武汉安恒信息科技有限公司自成立以来，在彭建军同志的带领下已助力湖北省公安厅、省医保局、省卫健委、第七届世界军人运动会网络和信息安全保障、武汉市委网信办、市公安局、市人力资源和社会保障局、东风汽车集团股份有限公司、汉阳区人才服务中心、汉阳区企业服务中心、汉阳区大数据中心等多个信息化安全项目落地建设，为武汉市网络安全建设、数据安全建设、密码应用建设、智慧应用建设、安全运营等方面做出了重要贡献，推动了武汉数字经济高质量发展。

2019 年第七届世界军人运动会在武汉举行，来自 109 个国家的 9300 余名军体健儿同场竞技。这是中国第一次承办综合性国际军事体育赛事，也是继北京奥运会后中国举办的规模最大的国际体育盛会。安恒信息作为武汉军运会馆方独家网络安全服务商，全面负责武汉军运会全程网络安全保障工作，为云平台、竞赛信息系统、竞赛场馆网络、转播网络、主媒体中心、军运村、开幕式及闭幕式场地的安全运行提供网络安全保障；同时还作为武汉市公安局军运会网络安全保障核心支撑单位，是武汉军运会期间全市重点系统网络安保的坚实力量。作为项目负责人，从筹备到建设，他全程参与，不舍昼夜，组织协调多方资源开展军运会信息基础设施现场安全检查服务及互联网信息系统安全监测服务。我们以专人专岗、实时响应，7 × 24 小时现场值守，实现了武汉军运会“零安全事件”的保障目标。

同时作为政协委员，他积极下沉挂点社区，进行反诈宣传，提高群众防范诈骗的意识和能力，共同守护居民财产安全。

彭建军同志愿下好“先手棋”、筑牢“防火墙”、加上“安全锁”，带领安恒信息做好华中网络安全的守卫者！

（供稿：安恒信息　贾高彦）

优秀工作者｜李荣
——把握机遇，逐梦前行

随着互联网技术的飞速发展和普及，网络已经成为人们生活、学习和工作中不可或缺的一部分。它不仅极大地便利了人们的日常生活，也推动了社会生产力的进步和经济结构的转型。与此同时，网络安全问题亦日益凸显，成为影响国家安全、社会稳定以及人民群众利益的重要因素。

在武汉这座蓬勃发展的城市，有一位致力于网络安全领域的工作者，不仅勤奋工作，而且持续学习，在不断地深化网络安全理论知识和实践技能的同时，运用他的专业技能为维护网络环境的安全稳固贡献着自己的力量。

他就是李荣。

李荣，出生于 1980 年，作为一名专业的网络安全专家，而今不惑之年的他已经在网络安全领悟有着二十余年的经验。自大学毕业后，他先后从事过信息系统自动化运维、驱动开发、渗透测试等工作，于 2017 年加入湖北省东方网盾信息安全技术有限公司后，他专职从事网络安全测评工作至今。

在李荣的职业生涯中，他深知网络安全技术领域的知识更新迅速，所以始终坚持持续学习，保持着学习新知识和技能的热情，不断提高自己的专业能力，他对网络安全工作充满热情、认真负责，始终将测评质量、用户满意度放在首位，致力于为用户的网络安全提供最优质的服务。

李荣在工作中始终坚守东方网盾的价值理念——“守正、创新、团结、共赢”，以高度的责任心和使命感投入到网络安全工作中。他恪守正道、不忘初心，抱着对工作负责，对用户负责，以用户为中心的态度，以提升团队技术水平、提升用户满意度作为永恒的目标，持续为用户的网络安全工作贡献自己的一份心一份力。

目前，李荣在湖北省东方网盾信息安全技术有限公司主要负责公司的网络安全等级保护测评团队、商用密码应用安全性评估团队、软件测试团队的技术管理工作。在他和团队的共同努力下，东方网盾荣获年度测评机构能力验证优秀单位、首届“熵密杯”密码应用安全竞赛优胜奖、信息安全性测试能力验证“优秀实验室”等荣誉。

李荣始终秉承“学无止境”的观念，致力于个人技能和知识的不断提升，通过不懈的努力，他取得了一系列重要的专业认证，如 CISP、CISP-PTE、CISSP、CISA 等，

涵盖了信息安全、渗透测试、系统安全以及信息系统审计等多个关键领域。除此之外，李荣还具备商用密码应用安全性评估、网络安全等级保护测评、高级信息系统项目管理和高级网络规划设计等各领域的资格证书。这些严格的认证不仅证明了他的专业知识水平，也体现了他对网络安全领域的全面理解和实践能力。

他带领网盾技术团队为用户提供优质的网络安全服务，协助用户制定网络安全策略、实施网络安全措施、进行网络安全审计等工作，保护用户信息系统和数据安全。在用户碰到网络安全相关的疑难杂症时，他总是带领公司网络安全团队第一时间赶到现场，协助用户迅速查明事件原因，采取有效措施防止事态扩大。他曾协助用户成功处置过多起网络安全事件，为保障用户的信息系统安全稳定运行做出了应有的贡献。

在配合行业主管部门进行网络安全检查时，李荣总是认真履行职责，协调公司资源、抽调精兵强将，在检查中帮助企业、单位提高网络安全防护能力。他和网盾人都深知，坚持共赢、做好本职工作，才能协助行业主管部门、协助用户做好网络安全工作，才能从根本上保障网络安全。

作为一名网络安全工作者，李荣的故事提醒我们，网络安全背后是无数专业人士的辛勤付出和无声守护，他们始终坚守在网络安全的第一线，用实际行动为用户、为社会贡献着自己的力量。他用自己的事迹告诉我们，在平凡的岗位上也能创造出不平凡的业绩。他们是这个信息化时代不可或缺的英雄，用专业和热情确保了我们的数字生活更加安全和可靠！

（供稿：东方网盾　扈莎莎）

优秀工作者｜王志豪
——发扬铁脚板精神，冲锋网安领域

“铁脚板”是一种精神，是敢为人先、追求卓越的胆量，是任劳任怨、埋头骨干的执着，是勇于担当、肩负使命的气魄。“没有比人更高的山，没有比脚更长的路”，这是王志豪时常挂在嘴边的话。这句话，也是他奋战创新项目的真实写照。从 2011 年大学选择攻读网络信息安全专业开始，一份热忱的责任和担当陪伴他走过十余年的网安之路。

一、业务上，兢兢业业

强化建设重大项目，开拓网络安全市场份额：凭借专业的技术能力，他每年取得多个重大项目的签约落地，其中他参与的某设计院网站云安全防护项目，凭借其精湛的技术、专业的服务精神获得客户高度认可，并多年持续续约。

紧盯项目过程管理，打造高质量客户口碑：他坚持以目标管控为核心，盯过程管理、细节管理，其中他参与的某央企集团公司网络安全重保服务项目，在重点保障时期与客户一起坚持熬夜值守、并肩作战，其兢兢业业的工作态度获得了甲方感谢信。

善于总结发现问题，梳理项目管理规范：工作中，他克服了客户需求不明确、资料欠缺、客户原设计方案存在缺陷等各种困难，总结项目全生命周期的管理要点及流程，建立项目管理规范，为同类型项目落地树立典范。

二、态度上，精益求精

他能够结合业务需求规范，独立完成网络安全架构整体规划、与同事一起参与网络设备和安全设备等平台软硬件调试及上线工作，为公司节约项目成本。

他能够创新项目思维，提出安全软件开发类项目新思路，开创软件开发框架类的新形式，在方案内容上进行整理和延伸，帮助客户解决了潜在开发需求过多、具体需求尚不确定，且预算又有限的问题，顺利完成项目落地及交付。

他能够发现和消除各类安全风险隐患 30 多个，更正实施方案中存在的严重影响实施交付问题达 50 余个，修正和明确项目参数 100 余处，有效避免了各类损失和风险隐患。

三、服务上，面面俱到

他负责支撑武汉联通网络信息安全项目，对接全市所有行业营服与区县营服多达上百人客户经理。他有执行事前定规范、会议有纪要、工作常复盘的工作习惯，一线工作人员遇到任何网安项目的问题，他都耐心、热心、暖心为他人解决所有困惑，积极为一线减负，全力为一线赋能。他在岗位上默默耕耘、勤勤恳恳、平易近人，得到领导和同事们一致认可，在平凡的岗位上打造不平凡的口碑！

新时代的中国青年，生逢其时、重任在肩，施展才干的舞台无比广阔，实现梦想的前景无比光明。新时代的网安青年，既拥有广阔发展空间，也承载着伟大时代赋予的历史使命，致力于为武汉市网络安全业务发展贡献自己光和热！

（供稿：武汉联通 吴清林）

优秀工作者｜吴承鹗
——青春无悔，网络安全

在青春的璀璨年华里，我们铭记一句古老的箴言："青年强则国家强。"在这个信息爆炸的时代，网络安全的重要性不言而喻。它不仅是国家的屏障，更是民众的护盾。因此，培养精通此道的人才成为了国之大计、时代之问。

在湖北的武汉，有这么一个执着追求的守护者——吴成鹗。他是武汉艾迪时代网络技术有限公司网络安全部门的典范人物，自 2012 年起便与网络的丝线结下不解之缘，将青春与热血献给了这份高尚的事业。

他以专业的素养和对事业的无限忠诚，成就了非凡的职业道路。他的工作态度，如同古语所云："业精于勤，荒于嬉；行成于思，毁于随。"他在岗位上兢兢业业，不断推动网络安全教育的进步，致力于打造一代新的网络防线。

身为专家，吴成鹗以其深厚的行业知识与丰富的教学实践，参与塑造湖北高校的网络安全课程体系，为国家的未来把脉，为产业的需求输送血液。他所倡导的"现代学徒制人才培养模式"不仅创新教育思路，更为产教融合树立了新的典范。

他的公益精神，亦如星辰般熠熠闪光。无论是走进校园还是深入社区，他都不遗余力地向人们普及网络安全知识，提升公众的防护意识。他深知，个人的

吴承鹗组织学生参与军运会网络及信息安全保障工作

数据安全是构筑国家安全的第一道防线。

在众多荣誉背后，吴成鹗始终坚守初心，为学生授课时，他总是能够深度剖析网络安全的各个层面，从宏观到微观，为学子们描绘出一幅幅未来的蓝图。

吴成鹗，这位热心公益的卫士，用实际行动诠释了一个新时代网络安全工作者的使命与担当。他的故事，就是一曲关于坚守与奉献的赞歌，为我们构筑了一个更加安全、稳定、繁荣的网络世界，让青春无悔，让岁月静好。

在教育的天地里，吴成鹗如同一颗璀璨的星辰，照亮了无数学子的职业道路。他不仅在本职岗位上取得了令人瞩目的成就，更以一颗赤诚之心，积极参与到公益事业中，倾注全力于人才的培养。

他，立足岗位，勤恳敬业，凭借深邃的行业洞察力和丰富的实践智慧，为高校培养了一批又一批企业所需、时代所倚的网络安全精英。他引领团队创新推出“现代学徒制人才培养模式”，架起了产教结合的桥梁，为国家网络安全的未来铺设坚实的基石。

在举世瞩目的 2019 年军运会上，他组织带领学生投身于网络安全的第一线。他不仅是知识的传播者，更是实践的引路人，让学生们在实际项目中磨砺技能，也让企业在激烈的竞争中发现未来的希望。

他的热心不只停留在课堂上，更延伸至社区，以至每一个角落。他深知网络的海洋浩瀚而深邃，需要每一个人的守护和贡献。因此，他将网络安全的重要性传遍每个听众的心田，提升公众的防范意识。

从国家到社会，从企业到个人，他在“生科”、“襄汽”、“武信”等多座学府讲授的“网络安全第一课”中，为学子们勾勒出一幅清晰的职业发展蓝图。他不仅是一位实干家，也是育人为先的教育者。

同时，吴成鹗和他的公司武汉艾迪时代网络技术有限公司同事们积极投入“楚慧杯”、“黄鹤杯”等公益赛事中，为国家大型活动的成功举办提供坚实的保障。

在新时代的征程上，吴成鹗这位热血的网络安全专家，以行动诠释了网络战士的责任与担当，为建设一个更加安全、稳健和繁荣的网络世界不懈奋斗。

（供稿：艾迪时代 向杰）

优秀工作者｜向仕华
——锐意进取，勇攀创新高峰

作为一名共产党员，向仕华同志一如既往地把高标准、严要求贯穿工作的始终，发挥党员同志敢闯敢拼、率先垂范的精神，以“固不可破”的锐气应对复杂局面，以“叩石垦壤”的志气开拓创新，勇攀创新发展的高峰。

创新研发无止境，推广应用不停步。自参加工作以来，向仕华便一直深耕于智能建造领域。从事智能建造相关工作近 10 年以来，他主导武汉市汉阳市政建设集团有限公司智慧化、数字化、信息化项目的建设工作，先后主导建设“筑建通施工现场管理系统、机械指挥官平台、材料采购订单系统、视频监控平台、智能安全帽平台、移动加油宝平台、工程类智慧报表系统、集团级数字工地平台”等共计 20 余款软件平台。他所参与的项目获得年度工程建设行业互联网发展最佳实践案例、全国建设业企业信息化建设优秀案例等奖项共计 11 余次，主持申报并取得 17 余项软件著作权，2 项专利权。

一往无前，深耕智能建造

近年来，国家大力推行智慧城市建设，武汉汇科智创科技有限公司作为汉阳市政集团战略布局数字化新业务板块的主要组成部分，在向仕华同志的带领下阔步向前，牢牢抓住新的历史机遇，在智能建造的版图上攻克一个又一个的难关，书写全新的篇章。

推进产业数字化、智能信息化建造。从 2021 年起，向仕华先后主持建设了武汉市汉阳区融媒体项目和青创园项目。融媒体项目包含演播室及周边配套区、融媒体指挥中心（兼具新闻发布厅）、融媒体业务平台等

八大核心区域。青创园项目承载展示 - 苗圃 - 众创空间 - 孵化器等功能。在项目推进过程中，向仕华带领团队以数字化、智能化赋能运营的基本要求，实现了项目的软硬一体化建设。

致力于建筑信息化创新发展研究。自接触建筑信息化行业以来，向仕华主导编制了建筑业施工企业数字化转型整体蓝图，打造集团公司 1+2+3+N 的数字化体系建设，逐步将传统建筑企业向数字化转型。目前致力于研究开发汉阳区城市信息模型（CIM）平台，积极组织设计开发汇报，希望后期能将城市信息模型打造成标杆项目。

主管集团公司 BIM 技术的推广应用。主导编制集团级 BIM 应用技术标准，指导 BIM 应用实施的项目，在此期间主导了武汉月亮湾城市阳台、高新三路提升改造工程、汉阳市政建设大厦等多个项目的 BIM 应用实施，主持的项目先后获得国家级、省市级协会奖项共计 23 个，其中国家级协会奖项有 14 个。

扬帆奋进，擘画时代蓝图

党的十八大以来，党中央高度重视科技创新，围绕实施创新驱动发展战略，加快推进以科技创新为核心的全面创新。新的时代，新的起点，坚定不移走创新之路，寻求建筑行业新的发展方向，依旧任重道远。

春风浩荡满目新，扬帆奋进正当时。智能化建造的蓝图已经绘就，前景无限光明。作为一名新时代的党员，作为智能化建造领域的开拓者，向仕华同志将以锐意创新的勇气，敢为人先的锐气，蓬勃向上的朝气，在创新发展的道路上锐意进取，勇毅笃行，以“领头雁”的果敢，“拓荒牛”的劲头，不断开创新局面，书写新高度，践行使命担当，擘画时代蓝图。

筑梦未来，践行责任担当

汲取榜样力量，对外推选汉阳楷模向仕华，发挥先进典型示范引领作用，以高质量文化精神赋能高质量发展。向仕华同志以身作则，发挥榜样的示范带动作用，积极带领团队参与各项社会志愿活动，疫情期间首当其冲作为志愿者参与下沉，空闲时间参与党员下沉履行社会职责，同时组织 [助苗计划] 第三期公益捐书活动，给贫困小孩送爱心，筑梦想。未来也将不忘初心，用行动诠释，在发展中扛起为社会贡献力量的旗帜。

（供稿：汇科智创　汪严明、王秋霞）

上图为向仕华参加工程建设行业互联网大会

优秀工作者｜张映
——用情怀和行动，守护网络安全

张映，北京天融信安全服务专家、网络安全意识培训讲师，湖北省信息网络安全协会培训讲师，湖北省财政厅信息化领域评审专家，《2021 网信自主创新调研报告》编委，《电子健康卡系统平台安全可靠运行技术要求》编委，信息系统项目管理师，网络安全应急响应工程师，注册信息安全工程师，毕业于四川大学，2012 年毕业至今致力于网络安全研究与建设，主导过多个企事业单位网络安全体系建设规划。圆满完成了第十四届湿地公约缔约方大会、党的二十大等重大活动安全保障任务。作为网络安全培训讲师，2021 年回汉至今，为长江水利委员会、湖北省环境科学研究院、武汉市卫健委、江汉水网、武汉市档案局等政府、企事业单位开展 30 余次网络安全意识培训及网络安全法律法规解读培训，培训人次达 1500 余人。张映主要先进事迹如下：

勤学习，履行自身职责的本领强实。夜深人静，在明亮的台灯下，张映打开了一本书，开始了每天一小时的学习。“学无止境，学以致用”是她的座右铭。深入学习领会习近平总书记网络强国重要思想，认真落实国家网络安全政策，认真学习《中华人民共和国网络安全法》《中华人民共和国数据安全法》《网络安全审查办法》等法律法规，力求准确把握网络安全工作面临的形势和任务。持续不懈加强业务学习，努力掌握网络安全领域的新知识、新技能，不断提升网络安全业务能力，积极参加网络安全领域认证考试培训，获得了网络安全应急响应工程师、注册信息安全工程师、关键信息基础设施安全防护专家等证书，努力成为本行业、本领域技术专家。

重实干，植根一线锤炼业务能力。“实践出真知，实践长真才”是张映始终贯彻的方针，多年来坚持在干中学、学中干，坚持知行合一、以知促行、以行求知，不断提升自己的本领水平，2022 年在武汉召开的第

十四届湿地公约缔约方大会，会议涉及范围广、级别高、议程长，网络安全形势严峻，张映作为项目经理，全身心投入到大会的筹备工作中，带领团队构建了资源、技术及应急三重网络安全保障框架，与会议相关的各方人员分工协作，会议期间有效防御了数十万次各类攻击，以“零事故”的成果保障了会议的正常进行。梳理出的大会保障流程、方案、思路等，为日后承办类似重大会议活动提供了成功的路径实践与经验积累。

勇担当，扎实有效推进全员安全意识提升工作。“网络安全为人民，网络安全靠人民”是国家 2015 年至今网络安全宣传周的主体，我国网络安全事业起步较晚，公众网络安全意识不足。张映作为网络安全从业者，以提升全民网络安全意识为己任，2021 年至今，始终走在安全意识宣贯的前线，深入开展网络安全进社区、进企业、进机关、进校园等多项重要活动，作为培训讲师开展了 30 余次网络安全意识培训及网络安全法律法规解读培训，培训人次达 1500 余人，让网络安全观念愈发深入人心，共筑网络安全“防火墙”。

网络安全工作没有终点，更多不可预见的挑战还在她前方的路上，但她时刻准备着，在这张由“0”和“1”构成的无形之网间，在这个没有硝烟但充满着警醒的战场中，用情怀和行动在网络安全领域不懈奋斗，用自己的方式为网络安全的发展贡献出了力量！

（供稿：天融信 吕露）

优秀工作者｜邓亚洲
——巨人背后的专家

2024 年 4 月，邓亚洲获得武汉市网络安全协会的颁发的 2023 年度优秀工作者称号，这是对他个人在过去一段时间来所做工作贡献的认可。作为绿盟科技湖北区域技术总监，他长期活跃在用户一线，为省市两级主管机构、关基运营单位以及其他面临网络安全威胁的单位提供技术服务，解决过诸多的技术难题。

绿盟科技是网络安全界的老牌名企，以技术人员专业精进闻名，业界号称“黄埔军校”。在绿盟湖北的技术团队中，老中青梯队层次明显，咨询专家、产品方案专家以及攻防专家结构合理，有浓厚的技术氛围，在公司内部的各种工作中获得荣誉奖项无数，是公司名副其实的“技术明星”团队。

秉持“来源于用户、服务于用户”的带队理念，邓亚洲始终要求团队成员以解决用户安全需求为第一准则，从用户需求中出发寻找技术创新点，然后推动绿盟武汉光谷研究所进行技术论证和开发，最后再将新技术或产品应用到用户场景中进行验证，不断迭代打磨出可以解决用户实际问题的产品功能。

2021 年，在武汉国家网络安全人才与创新基地举行的武汉科技成果转化对接活动·武汉临空港开发区（东西湖区）专场上，邓亚洲作为企业代表，现场向与会领导和嘉宾分享了绿盟与与华中科技大学共建的黄鹤靶场，该靶场主要是围绕人才培养、攻防竞技、前沿技术科研等方面进行设计，满足学校在实训授课、实验实践、仿真场景训练等多方面的需求，帮助高校培养网络安全攻防实战型人才，是绿盟武研所近年来重点打磨的一款

综合性网络安全平台，具备行业领先的技术水准。

该靶场是典型的需求来源于用户、创新服务于用户的成功范例，目前已投入使用 3 年有余，承接了多次网络安全竞赛活动。如 2023 年第二次承接全国大学生信息安全竞赛创新实践能力赛华中赛区决赛，一共有 30 余所高校的 80 支参赛队伍、300 余名学生参加比赛，2023 年由武汉市网络安全协会和绿盟科技等共同协办的 2023 黄鹤杯网络安全人才创新大赛等。

同时，绿盟湖北区域还研发了全流量分析系统、固件安全分析系统、物联网风控平台、互联网反诈平台、车联网安全监测与防护系统、BOT 动态安全防护系统等多款贴合省内用户需求的产品，在一些运营商、金融、政企等用户处实际应用生效。

这里也重点介绍一下绿盟武汉研究所，该所最早成立于 2011 年，目前是国内网安公司在武汉规模最大的研发机构，吸纳了一大批华科、武汉理工等高校的毕业学子就业发展，取得多项发明专利以及产品软著成果，内部还设有顶尖的攻防战队和安全研究实验室，长期为省内用户提供技术力量支撑。

在未来，邓亚洲将带领绿盟湖北区域技术团队继续迎接网络空间安全最新挑战，追踪业界安全趋势，不断学习、不断进步，贴合用户业务场景，打磨出更好用的网络安全产品，实现用户价值与公司价值的双赢，为武汉市网络安全防护体系的建设做出更大的贡献。

（供稿：神州绿盟 陈爱珍）

我会《数据要素场内流通安全评估技术规范》团体标准编制工作正式启动

2024 年 1 月 9 日，由武汉市网络安全协会主办、武汉安恒信息科技有限公司支持并承办的《数据要素场内流通安全评估技术规范》团体标准启动会在安恒华中总部网络安全基地万科未来中心召开。

随着数据成为驱动经济社会发展的关键生产要素，保障数据要素的安全流通变得愈发重要。习近平总书记指出，要构建以数据为关键要素的数字经济，维护国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济。

在此背景下，本次启动的《数据要素场内流通安全评估技术规范》团体标准由武汉安恒信息科技有限公司提出，武汉市网络安全协会归口，并已通过全国团体标准信息平台立项审核并公示。会议由牵头单位武汉安恒信息科技有限公司总经理彭建军主持。

武汉大学国家网络安全学院张立强教授在会议中表示，数据要素场内流通安全评估技术规范是确保数据要素在特定场内流通的安全性和合规性的重要标准，团体标准规范的制定对组织机构数据要素场内流通的安全性，保护数据的机密性、完整性和可用性非常有价值。同时，也有助于组织机构符合相关法律法规和标准的要求，降低因数据泄露或违规操作带来的风险和损失。

武汉市网络安全协会相关负责人向与会代表介绍了协会标准化工作的有关情况，并对本项团体标准的

立项背景和有关法规的理解做了说明。

代表们详细讨论了本项团体标准目标、范围、预期效果、文本结构、工作计划与分工等标准编制具体工作。汉阳区大数据中心黄颖倩、杨建平，中国长江电力股份有限公司张辉，长江水利委员会水文局邹冰玉、刘迪，武汉大学国家网络安全学院张立强，湖北数据集团有限公司古伟，武汉网络安全技术有限公司孙进，武汉趣链数字科技有限公司李宏民，武汉安恒信息科技有限公司彭建军、邓浩等编制组专家代表分别对标准结构和内容进行了深入的讨论并提出了专业建议。

会议决定，根据《国家标准化法》、《国家团体标准管理规定》和武网安协《团体标准管理办法》有关规定，结合会议讨论的意见和建议，进一步修订工作计划，分步启动标准起草、调研和编制工作。

该标准将聚焦数据要素领域，通过联合“政产学研用”各类机构，汇聚数据要素与数据安全领域头部单位和学者，共同研究编制，期望通过本标准的编制和推广工作达到建立数据来源可确认、使用范围可界定、流通过程可追溯、安全风险可防范的数据可信流通评估体系，为有序发展场内数据流通和交易开展标准探索。

武汉市网络安全协会将继续联合武汉安恒信息科技有限公司，支持本项团体标准编制工作组的各项工作，积极协调各方资源，广泛邀请有技术实力和意愿的单位及专家参与，深入调查分析，严控标准编制规范，增强本标准的代表性、科学性与合理性，坚决筑牢网络安全屏障，保障关键信息基础设施安全，强化网络安全保障，不断提升我市安全保障水平和安全发展能力。

网络安全相关标准制定服务

武汉市网络安全协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。

联 系 人：乔老师

联系电话：027-82757716

我会《网络安全人才实战化训练环境建设》团体标准编撰研讨会（第一次）顺利召开

3 月 29 日，武汉市网络安全协会《网络安全人才实战化训练环境建设》团体标准编撰研讨会（第一次）在奇安信集团湖北分公司召开，该标准于 2023 年 6 月通过武汉市网络安全协会立项审查，由奇安信科技集团股份有限公司（以下简称“奇安信”）牵头起草。来自全市本科、高职院校及相关企业等专家围绕《网络安全人才实战化训练环境建设》标准框架及主要内容，开展了深入研讨。

会上，标准牵头单位奇安信公司首先介绍了标准的立项背景及意义、标准适用范围、主要技术内容以及下一步工作计划。武汉市网络安全协会标准工作部主任乔奇向与会专家对标准制定的支持表达了衷心的感谢，希望各位行业专家继续支持协会标准工作。来自湖北经济学院、武汉职业技术学院、武汉软件工程职业学院、湖北科技职业学院、武汉商贸职业学院、湖北国土资源职业学院、武汉交通职业学院、长江职业学院等专家们围绕标准技术内容进行了细致深入地讨论，对该标准的相关内容提出了诸多宝贵的意见和建议。

下一步，团体标准工作组将认真梳理和研究各位专家的建议，发挥各参与单位的优势，凝聚合力，对标准内容进行进一步优化完善，不断提升标准的制定水平。

我会入选湖北省第一批优质团体标准制定主体重点培育名单

近日，湖北省市场监督管理局联合其他九个相关部门印发了《关于实施以标准升级服务保障大规模设备更新和消费品以旧换新行动的工作方案》的通知。

本方案中决定实施团体标准培优计划。要求加强政策支持和指导协调，推出指导制定、实施、修订团体标准的具体措施，协调各有关行政主管部门加大政策支持力度，聚焦产品服务质量提升，规划团体标准培优项目库。在“两新”相关领域重点培育 50 家具有影响力的优质行业协会、学会、产业技术联盟等团体标准制定主体（第一批重点培育主体 33 家，见附件 5），响应生产和消费需求，及时制定发布体现湖北产业技术优势的团体标准。

在湖北省第一批优质团体标准制定主体重点培育名单中，我会成功入选。

未来，我会按照国家标准化法规要求和我省工作方案精神，不断加大高质量优质团体标准供给，带领广大会员为省市网络安全标准化工作提供有力支撑、服务和保障。


附件 5

第一批优质团体标准制定主体重点培育名单

序号	团标主体	指导部门
1		
2		
3		
4		
5		
6		
7		
8		

我会率队拜访武汉理工大学管理学院并开展交流座谈

2024 年 2 月 29 日，我会携部分理事单位和会员单位代表拜访武汉理工大学管理学院，与学院领导和教师进行了深入工作交流。共同探讨网络安全与信息管理等专业领域的最新发展、企业用人需求以及校企合作机制等问题。会议由管理科学与信息管理系主任江长斌副教授主持。

管理学院党委杨伟波副书记代表学院热烈欢迎武汉网安协会一行，详细介绍了学院的基本情况和学科发展方向。他强调，管理学院一直致力于培养具有创新精神和实践能力的高素质人才，希望与武汉市网络安全协会所有会员加强合作，共同推动湖北武汉网络安全事业高质量发展。

信管系专业负责人王虎教授详细介绍了信管系的专业设置、师资力量、科研成果以及人才培养等方面的情况。据介绍，武汉理工大学管理学院办学历史悠久，始建于 1964 年，1965 年开始招收本科生，1981 年开始招收硕士研究生，1993 年获批管理科学与工程学科博士点，是国内管理学科起步最早的院系之一，信管系作为国家一流本科专业建设点，培养了大批拥有扎实计算机学科基础和经济管理知识的复合型人才，希望与武汉网安协会加强沟通合作，共同推进网络安全和信息化管理类人才的培养工作。

武汉市网络安全协会秘书长刘悦恒对学院的热情接待表示感谢。他表示，近年来，国家高度重视网络

安全工作，习近平总书记明确指出，建设网络强国需要高素质的网络安全和信息化人才队伍。武汉在国家网络安全事业版图中占据着极为特殊的地位，拥有全国首个国家网络安全人才与创新基地。当前，随着数字经济的高速发展，网络安全的内涵和外延也得到充分扩展，网络安全已经不是单纯的技术问题，而是涵盖网络空间和社会各方面的综合性治理课题。武汉网安协会愿意积极发挥桥梁纽带作用与理工大管理学院等高校加强合作积极探索，为政府、企业、高校等多方提供交流互动合作平台，共同推进网络安全产业技术教育融合发展。

随后，协会理事单位武汉数智云科技有限公司和会员单位浙江远算科技有限公司的负责人分别介绍了各自企业的基本情况、用人需求以及未来发展方向。他们表示，随着网络安全领域的不断发展，企业对网络安全人才的需求越来越大，希望与理工大加强合作，共同培养符合企业需求的高素质人才。

在自由交流环节，与会人员就校企合作和联合培养、重点课题攻关等工作进行了深入的探讨和交流。

本次活动不仅加强了各方的深入了解，也为未来的校、行、企深入合作奠定了基础。各方将在人才培养、创新研究等方面开展积极努力和务实合作。

我会组织召开武汉市 2024 年网络安全技术人才职称评审工作政策宣贯会

为深入贯彻落实国家关于加强网络安全人才培养工作的各项要求，推动武汉市网络安全技术人才职称评审工作规范有序开展，进一步提升专业技术人员的能力和水平，武汉市相关部门于 3 月 15 日联合举办了 2024 年网络安全技术人才专场职称评审工作政策宣贯会。

本次宣贯会由市人社局和市委网信办的共同指导，市人事考试院提供支持，市网络安全协会承办。会议邀请了市委网信办、市人社局、市人事考试院等相关领导及专家出席，市网安协会三十余家会员单位负责人和人事负责人参会。

在会议上，主持人首先阐明了本次宣贯会的背景及目的，强调了职称评审工作在网络安全专业技术人才培养与发展中的关键性地位。紧接着，市人社局专业技术人员管理处二级调研员王金舟对武汉市今年职称评审政策进行了深入细致的解读，使与会人员全面、准确地把握了政策精神与要求。市人事考试院的钟老师随后对职称申报的详细流程进行了系统梳理，并对注意事项进行了逐项说明，为申报人员提供了具有操作性的指导。最后，市人事考试院评审部部长冯燕针对申报工作提出了明确要求，进一步确保了评审工作的公正性与严肃性。

武汉作为国家网络安全人才与创新基地的承载地，一直高度重视网络安全工作。此次针对网络安全民营企业专业技术人才开展的专场培训及评审工作，是武汉市加强网络安全人才培养和管理的又一重要举措。通过本次宣贯会，与会人员不仅深入了解了职称评审政策，也为我市网络安全领域人才提供了及时、有效的政策信息和评价支持。同时，会议还设置了答疑环节，与会人员就申报及政策相关问题进行了深入交流和探讨。

本次宣贯会的成功举办，将进一步推动我市网络安全领域人才职称评审工作的规范化、专业化发展，提升网络安全技术人才的专业素质和创新能力，为武汉市网络安全事业的持续健康发展提供坚实的人才保障。

武汉市网络安全协会第二届理事会第四次会议顺利召开

2024 年 3 月 21 日上午，武汉市网络安全协会第二届理事会第四次会议在武汉会议中心顺利召开。

本次大会 31 名协会理事单位和监事代表参与了会议。会议由协会理事长潘宣辰主持，武汉市委网信办网络安全处到场指导。

首先，协会秘书处就 2023 年协会工作概况、财务状况及 2024 年重点工作计划向理事会作出汇报。在主管部门的指导下，秘书处 2023 年攻坚克难，锐意进取，不断开创新局面，持续书写发展新篇章。我们紧密围绕我市网信中心任务，积极支持主管部门工作，竭诚服务广大会员，取得了显著成效。

在会议上，经过认真审议，与会代表一致通过了以下议题：《协会拟增相关工作制度》、《协会理事会拟更新名单》、《武汉市网络安全协会安全保险工作委员会

工作条例》、《武汉市网络安全协会网络安全保险工作委员会负责人及委员提名名单》、《武汉市网络安全协会民办高校工作委员会工作条例》、《武汉市网络安全协会民办高校工作委员会负责人及委员提名名单》、《协

会第四批专家委员会专家名单》、《2023 年武汉市网络安全协会优秀会员单位及优秀工作者名单》。同时，会议还审议通过了《关于协会投资成立网络安全服务实体机构的提案》和《关于召开第二届第二次会员大会的议案》。这些议题的通过，将为协会未来的工作提供有力的制度保障和组织支持，为推动我市网络安全事业的发展注入新的动力。

在会议中，理事们认真听取了关于 2023 年度立项团体标准工作的进展情况汇报，并研究了 2024 年度轮值会长的工作安排。同时，举行了 2024 年第一次轮值会长交接仪式，标志着新一轮值会长工作的正式启动。

在现场热烈的掌声中，武汉市网络安全协会第二届理事会第四次会议圆满结束。

新征程，新希望，未来“武汉网络安全”集体将在主管部门的指导下，携手前行，共同努力，为武汉网络安全事业做出更新更大贡献！

网络安全保险工作座谈会成功召开

为深入贯彻《网络安全法》《数据安全法》等相关法律法规，落实工业和信息化部、国家金融监督管理总局《关于促进网络安全保险规范健康发展的意见》要求，加快推进我省网络安全保险新模式落地应用，4 月 2 日，由湖北省经济和信息化厅主办，武汉市网络安全协会网络安全保险工作委员会承办的网络安全保险工作座谈会在洪山大厦成功召开。

协会会员、网安保险工委会成员、需求侧企业、网络安全企业、保险公司等单位共二十余家代表参加座谈，共同就拟定的网络安全保险试点方案、试点内容、工作流程等内容进行深入交流，听取各方的意见和建议。会议中，省经信厅信息化推进处吴欢处长对试点方案和具体工作提出了相关要求。

与会各方纷纷表示，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，大家愿在行业主管部门的指导支持下，协会及工委会的组织下，积极发挥各自专业优势，加强沟通协作，打通行业壁垒，创新服务模式，促进网络安全保险需求释放和应用示范落地。

湖北武汉拥有完整的现代产业基础、科教人才、交通区位等众多独特优势，拥有全国首个国家网络安全人才与创新基地，还拥有全国唯一的国家级科技保险示范区。去年初，武汉市网络安全协会率先全国启动网络安全保险领域的探索，与武汉东湖科技保险发展促进中心签订战略协议，共建“东湖网络安全保险服务中心”，启动相关标准研制，并成功落地多个网安保险案例，在刚刚结束的武汉市网络安全协会第二届第二次会员大会上，在省市主管部门的见证下，成立了华中首个网络安全保险工作委员会。

工委会将持续支撑省市主管部门，通过资源整合、平台支撑和标准赋能，做好会员企业与政府主管部门桥梁纽带，努力引导网络安全保险新兴领域工作健康有序发展，培育网络安全保险新业态，帮助企业加强网络安全风险管理，为推动湖北武汉网络安全产业高质量发展作出积极贡献。

武汉市网络安全协会联合多所院校组织开展全民国家安全教育日网络安全进校园主题教育活动

武汉软件职业学院

武汉商贸职业学院

武汉交通职业学院

湖北财税职业学院

4 月 15 日是第 9 个全民国家安全教育日，主题为“总体国家安全观 • 创新引领 10 周年”。为深入学习贯彻习近平关于总体国家安全观和网络强国重要思想，在市委网信办的统筹指导支持下，武汉市网络安全协会联合我市部分重点院校，针对在校师生开展了内容丰富的“全民国家安全教育日网络安全进校园活动”主题活动。

此次主题活动，由法律和行业专家组成宣讲团，分别走进了武汉软件工程职业学院、武汉商贸职业学院、武汉交通职业学院以及湖北财税职业学院等院校，为数千名师生带来了网络安全相关法律法规解读和产业技术趋势等专业课程。

法律专家姚盼律师，向师生详细解读了国家《网络安全法》等法规，从保障网络安全，维护网络空间主权和国家安全的方向，从立法过程，法规内容，监管体制等方面进行解答，并通过案例分享，帮助师生们更好地理解网络安全法规的重要性和实际应用。

行业专家丁鹏详细讲解了电信诈骗套路及防范要点，密码保护及设置强口令密码的方法，他强调要始终加强自我保护，远离网络谣言及恶意软件，不断提

姚盼　泰和泰（武汉）律师事务所

丁鹏　武汉艾迪时代网络技术有限公司

刘悦恒　武汉市网络安全协会党支部书记、秘书长

升防范意识。

市网络安全协会党支部书记、秘书长刘悦恒向各学校师生介绍了全球网络安全现状和我国网络安全产业情况，对行业面临的挑战、近年来国家网安政策、技术趋势和需求进行了分析和展望，还与师生进行了知识问答和互动交流。

活动中，武汉软件工程职业学院党委副书记、校长蒋兴鹏表示，网络安全作为网络强国、数字中国的底座，将在未来的发展中承担托底的重担，是我国现代化产业体系中不可或缺的部分。师生应积极投身于学习和思考，不断提高国家安全意识，并增强防范及抵御安全风险的能力；武汉商贸职业学院校党委书记丁振国表示，学校应紧扣国家安全教育这一重点工作，牢记立德树人根本任务，持续推进国家安全教育宣传进校园，切实增强大学生国家安全意识；武汉交通职业学院电子与信息工程学院院长胡迎九表示，高校担负着为国家培养人才的重要任务，国家安全教育的前沿阵地，学校高度就是国家安全观教育和网络安全保障，加强网络安全教育，健全网络安全监管机制，培养提升学生的网络安全意识和道德意识；湖北财税职业学院党委委员、副校长刘彩霞表示，网络安全人人有责，呼吁全校师生积极参与网络安全工作，提高网络安全意识，掌握网络安全技能，共同维护国家安全。

通过本次主题教育活动，进一步引导我市师生自觉强化总体国家安全观，树牢网络安全风险防范意识，营造师生积极参与网络安全教育的良好氛围，为新质生产力筑牢人才和安全基石。

武汉软件工程职业学院党委副书记、校长 蒋兴鹏

武汉商贸职业学院校党委书记　丁振国

武汉交通职业学院电子与信息工程学院院长 胡迎九

湖北财税职业学院党委委员、副校长 刘彩霞

我会率队走访理事单位
——中国电信武汉分公司

为了深入了解协会会员单位实际经营情况，及时传达中央省市及主管部门相关政策，学习优秀成员单位的先进管理经验和技术服务模式，围绕成员单位在网络安全事业发展中遇到的需求和问题进行交流，不断提升协会服务能力。近日，武汉市网络安全协会秘书处与智能汽车网络安全专委会、网络安全保险工委会负责人一行，到协会理事单位——中国电信股份有限公司武汉分公司进行拜访交流并座谈。

中国电信股份有限公司武汉分公司副总经理覃兵代表公司热烈欢迎武汉网安协会一行，详细介绍了公司基本情况以及“五张网”、“一朵云”、“算力”新基建等领域的优势和应用案例，展示了其在信息化建设和网络安全方面的综合实力，并表示希望与武汉市网络安全协会及成员单位加强合作，共同推动武汉网络安全事业高质量发展。

武汉市网络安全协会秘书长刘悦恒对武汉电信的热情接待表示感谢。他表示，武汉电信作为全市信息化建设及关键信息基础设施的主力军，是构建全市网络安全屏障的中坚力量，非常荣幸邀请武汉电信加入到协会本届理事会行列，欢迎电信积极建言献策，参与协会治理，发挥理事作用。武汉市网络安全协会将充分发挥桥梁纽带作用，整合会员单位和分支机构资源，进一步加强双方合作，愿在党建活动、社会服务、赛会活动、标准制定、成果转化、各专业（工作）委员会建设等方面开展深入合作。

在自由交流环节，与会人员就网络安全保险落地推广、智能汽车网络安全及算力保障、智慧校园网络安全等工作进行了深入的探讨和交流。

在未来的发展道路上，武汉市网络安全协会将继续携手理事会员单位和合作伙伴，以合作共赢为目标，以科技创新为引领，以网络安全为基石，为培育发展新质生产力提供有力支撑。

中国电信股份有限公司武汉分公司党政客户服务部总经理刘学民、政企智能服务运营中心总经理向艳梅、党政客户服务部副总经理王欢、校园客户服务部副总经理陈昱泉、金融客户服务部总监杨帆、智能云网调度运营中心总监王蓉蓉、武汉市网络安全协会办公室主任张玉萍、政企服务部主任乔奇、公共关系部主任严媛、智能汽车网络安全专业委员会秘书长郝晓峰、网络安全保险工作委员会秘书长周韬参加本次活动。

我会智能汽车专委会 2024 年首次工作会顺利召开

武汉市网络安全协会智能汽车专委会召开 2024 年首次工作会议，聚焦智能汽车网络安全发展。

在智能汽车网络安全风险日益受到国家高度关注的背景下，武汉市作为我国汽车产业的重要基地，正积极利用自身产业优势，全力推动智能网联汽车产业高质量发展。为贯彻落实国家主管部门关于智能汽车网络安全的各项文件精神，武汉市网络安全协会智能汽车网络安全专业委员会（以下简称“专委会”）于 5 月 16 日在国家网络安全人才与创新基地天融信大厦成功召开了 2024 年首次工作会议。

本次会议汇聚了专委会成员单位及《车联网安全检测技术要求》团体标准参编单位等二十余家单位的代表，共同为智能汽车网络安全领域的发展献计献策。会议由专委会秘书长郝晓峰主持。

会上，郝晓峰秘书长首先汇报了专委会过去一年的工作成果及与国家相关机构的沟通进展，并建议未来专委会将在汽车工业设计安全领域深化研究与实践。随后，专委会围绕 2024 年成员纳新计划进行了深入探讨，明确了将重点吸纳在智能汽车网络安全领域有突出贡献的单位，共同拓展在汽车主机厂配套上下游、智慧物流、车路协同等领域的机构合作。

此外，天融信公司高级工程师刘鹏作为专委会副

主任单位代表，为与会人员带来了《车联网监管和数据安全要点解读》的专题报告，深入分析了当前车联网和数据安全领域的研究热点与政策趋势，为行业发展提供了宝贵的参考。

会议的另一重要议程是对智能汽车供应链安全问题进行了深入研讨，并对《车联网安全检测技术要求》团体标准和地方标准的编制工作进行了再部署，确保标准的科学性与实用性，为行业健康发展提供有力支撑。

最后，协会秘书长刘悦恒与副会长单位代表左世涛共同为专委会成员单位进行了授牌。武汉大学国家网络安全学院、湖北大学网络空间安全学院、东风悦享科技有限公司、湖北天融信网络安全技术有限公司、中国联合网络通信有限公司武汉市分公司、湖北省电子信息产品质量监督检验院、中汽研汽车检验中心（武汉）有限公司、神州绿盟武汉科技有限公司、武汉安恒信息科技有限公司、湖北珞格科技发展有限公司、开源网安物联网技术（武汉）有限公司、广电计量检测（武汉）有限公司、远江盛邦（北京）网络安全科技股份有限公司、东风商用车有限公司、襄阳达安汽车检测中心有限公司、猛士汽车科技公司等代表出席了本次会议。

会议在热烈的讨论和深入的交流中圆满落幕。

新增会员介绍

新晋理事单位：

中国电信股份有限公司武汉分公司于 2004 年 4 月 30 日成立，公司地址武汉市武昌区洪山路 1 号。主要营业范围，基础电信业务：增值电信业务：IPTV 传输服务：服务内容为 IPTV 集成播控平台与电视用户端之间提供信号传输和相应技术保障，传输网络为利用固定通信网络（含互联网）架设 IPTV 信号专用传输网络，IPTV 传输服务在限定的地域范围内开展；测绘服务：经营与通信及信息业务相关的系统集成、技术开发、技术服务、技术咨询、信息咨询、设备及计算机软硬件等的生产、销售、安装和设计与施工；房屋租赁：通信设施租赁：安全技术防范系统的设计、施工和维修：广告业务。（市场主体依法自主选择经营项目，开展经营活动：依法须经批准的项目，经相关部门批准后依批准的内容开展经营活动；不得从事国家和本市产业政策禁止和限制类项目的经营活动。

新增会员单位：

武汉网信联盾网络安全技术中心（有限合伙）

中心总部 2018 年 9 月 17 日注册于“国家网安基地”武汉临空港经济技术开发区。致力于网络安全空间安全、IT 治理、信息安全、IT 风险管理、IT 服务，始终以培养国内网络安全专业人才、组织网络安全人才交流为发展目标。专注于为政府、公安、运营商、高校、金融、能源、教育、企业、医疗等行业用户提供新一代安全解决方案。业务覆盖信息安全产品、信息安全集成、信息安全服务、信息安全培训四大模块，为客户的网络、业务提供高效、稳定的安全防护，帮助客户降低安全风险创造业务价值。公司创始人团队来自于国内顶尖数据通信、网络安全厂商高管及研发主管，其中多人拥有 CISP、CISSP、ITSS 及各大主流厂家安全认证。

武汉粟泰信息科技有限公司

武汉粟泰信息科技有限公司成立于 2018 年长期以来关注客户机房能效，为客户提供完整的网络能源产品，致力于成为机房数据中心及关键设备负载服务的优质供应商。公司与艾特网能等品牌厂家进行深度合作，作为艾特网能钻石代理商，一直以来与合作伙伴保持良好的沟通，秉承共进共赢的经营理念。公司业务主要包括模块化机房、UPS 不间断电源、蓄电池、精密空调、配电柜、发电机等机房基础设施产品的销售、安装、维护、保养，同时为顺应行业趋势，扩充产品的多元性，给客户提供更全面的服务体验，公司致力于网络安全领域业务的拓展，为客户提供机房一体化整体解决方案。

武汉中昊空间科技有限公司

武汉中昊空间科技有限公司属于科技型技术企业，增值税一般纳税人，于 2019 年 01 月 22 日成立，是以数据处理服务、影视动画服务、软件研发为主的公司，注册资本 500 万元，坐落于武汉市武昌区桃源国际写字楼 A 座 13A。多年来，我们在环保、交通、电力、水利等行业积累了丰富的经验，具备在智慧城市、智慧机场、智慧园区、智慧交通、智慧应急等多个领域提供完善解决方案的能力。公司向政府和企业客户提供专业的技术支持，赢得了广大客户的信赖和满意。

中国人民财产保险股份有限公司武汉市分公司

人保财险武汉市分公司是中国人保财险在武汉的分支机构，成立于 2003 年 12 月 18 日，总部位于于汉阳大道 408 号万科未来中心，作为系统副省级城市分公司，现内设 19 个部门、31 家经营机构、14 个城市社区服务网点、26 个农村营销服务部、2245 个三农服务网点。主要经营范围：财产损失保险、责任保险、信用保险、意外伤保险、短期健康保险、保证保险等人民币或外币保险业务，与上述业务相关的再保险业务，各类财产保险、意外伤害保险、短期健康保险及其再保险的服务与咨询业务：代理保险机构办理有关业务；经保险监督管理机构批准的其他业务。

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：湖北省武汉市江岸区兰陵路 2 号
电话：027—82757716　网址：www.whcsa.org.cn　邮箱 :hz@whcsa.org.cn