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

No network security　There is no national 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

武汉网络安全

WUHAN NETWORK SECURITY

武汉市网络安全协会通讯
2023年第1期　总第1期

内部资料　会员赠阅

WHCSA
武汉市网络安全协会
Wuhan Cyber Security Association

武汉市网络安全协会简介

INTRODUCTION TO WUHAN NETWORK 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。

武网安协具备全国团体标准信息平台团体标准发布单位资格；主办有全国首个“移动应用安全公益检测平台”；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”；是中国网络安全产业联盟授权的“网络安全优秀创新成果大赛”分站赛事华中地区承办单位；是武汉市互联网行业联合会副会长单位；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。

协会还带领成员单位参与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；主办承办各类型专业性论坛、赛事等大型活动；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。

作为拥有全国唯一的“国家网络安全人才与创新基地”的超大型国家中心城市—武汉，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！

会长寄语

2022 年是是极不平凡、具有里程碑意义的一年。武汉市网络安全协会在武汉市委网信办的领导和支持下，协助开展了武汉市国家网络安全宣传周系列活动、两江四岸灯光秀网络安全宣传活动、武汉市网络安全攻防演练、网络安全大讲堂等重要活动，还组织广大会员参加了多项团体标准编制、人才培养、课题研究和专业赛事工作。在此期间，得到了您的大力支持和帮助，共同为武汉市网络安全与信息化建设做出了贡献，在此表示衷心感谢！

2023 年，衷心期待协会会员、各位专家一如既往关心支持武汉网络安全发展，把家国情怀、事业理想、自我追求融入全市网络安全产业高质量发展、创新驱动发展的生动实践。

热忱希望更多在武汉发展的网络安全企业、从业人员、专家学者加入到武汉市网络安全协会这个大家庭，勇立潮头向未来，踵事增华再出发，为奋力打造武汉新时代英雄城市汇聚磅礴力量。

武汉市网络安全协会会长

潘宣辰

潘宣辰 中共党员

（武汉市网络安全协会会长、安天科技集团执行总裁，共青团武汉市委员会兼职副书记、武汉市洪山区第十五届、十六届人大代表、武汉大学兼职研究员、华中科技大学兼职教授）

目 录

CATALOGUE

工业和信息化部等十六部门关于促进数据安全产业发展的指导意见

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门、网信办、发展改革委、教育厅（委、局）、科技厅（委、局）、公安厅（局）、国家安全厅（局）、财政厅（局）、人力资源社会保障厅（局）、国资委、税务局、市场监督管理局（委、厅）、知识产权局，各省、自治区、直辖市通信管理局，中国人民银行各分行、营业管理部、各省会（首府）城市中心支行，各银保监局，各证监局，有关企业：

数据安全产业是为保障数据持续处于有效保护、合法利用、有序流动状态提供技术、产品和服务的新兴业态。为贯彻落实《中华人民共和国数据安全法》，推动数据安全产业高质量发展，提高各行业各领域数据安全保障能力，加速数据要素市场培育和价值释放，夯实数字中国建设和数字经济发展基础，制定本意见。

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，立足新发展阶段，完整、准确、全面贯彻新发展理念，构建新发展格局，坚定不移贯彻总体国家安全观，统筹发展和安全，把握数字化发展机遇，以全面提升数据安全产业供给能力为主线，以创新为动力、需求为导向、人才为根本，加强核心技术攻关，加快补齐短板，促进各领域深度应用，发展数据安全服务，构建繁荣产业生态，推动数据安全产业高质量发展，全面加强数据安全产业体系和能力，夯实数据安全治理基础，促进以数据为关键要素的数字经济健康快速发展。

（二）基本原则。坚持创新驱动，强化企业创新主体地位，优化创新资源要素配置，激发各类市场主体创新活力。坚持以人为本，维护人民数据安全合法权益，依靠人民智慧发展产业，发展成果更多更公平惠及人民。坚持需求牵引，以有效需求引领产业供给，以深度应用促进迭代升级。坚持开放协同，注重更大范围、更宽领域、更深层次的开放合作，协同推进全产业链深度融合、共创共享。

（三）发展目标。到 2025 年，数据安全产业基础能力和综合实力明显增强。产业生态和创新体系初步建立，标准供给结构和覆盖范围显著优化，产品和服务供给能力大幅提升，重点行业领域应用水平持续深化，人才培养体系基本形成。

——产业规模迅速扩大。数据安全产业规模超过 1500 亿元，年复合增长率超过 30%。

——核心技术创新突破。建成 5 个省部级及以上数据安全重点实验室，攻关一批数据安全重点技术和产品。

——应用推广成效显著。打造 8 个以上重点行业领域典型应用示范场景，推广一批优秀解决方案和试点示范案例。

——产业生态完备有序。建成 3-5 个国家数据安全产业园、10 个创新应用先进示范区，培育若干具有国际竞争力的龙头骨干企业、单项冠军企业和专精特新“小巨人”企业。

到 2035 年，数据安全产业进入繁荣成熟期。产业政策体系进一步健全，数据安全关键核心技术、重点产品发展水平和专业服务能力跻身世界先进行列，各领域数据安全应用意识和应用能力显著提高，涌现出一批具有国际竞争力的领军企业，产业人才规模与质量实现双提升，对数字中国建设和数字经济发展的支撑作用大幅提升。

二、提升产业创新能力

（四）加强核心技术攻关。推进新型计算模式和网络架构下数据安全基础理论和技术研究，支持后量子密码算法、密态计算等技术在数据安全产业的发展应用。优化升级数据识别、分类分级、数据脱敏、数据权限管理等共性基础技术，加强隐私计算、数据流转分析等关键技术攻关。研究大数据场景下轻量级安全传输存储、隐私合规检测、数据滥用分析等技术。建设和认定一批省部级及以上数据安全重点实验室，鼓励产学研用多方主体共建高水平研发机构、产业协同创新中心，开展技术攻关，推动成果转化。

（五）构建数据安全产品体系。加快发展数据资源管理、资源保护产品，重点提升智能化水平，加强数据质量评估、隐私计算等产品研发。发展面向重点行业领域特色需求的精细化、专业型数据安全产品，开发适合中小企业的解决方案和工具包，支持发展定制化、轻便化的个人数据安全防护产品。提升基础软硬件数据安全水平，推动数据安全产品与基础软硬件的适配发展，增强数据安全内生能力。

（六）布局新兴领域融合创新。加快数据安全技术与人工智能、大数据、区块链等新兴技术的交叉融合创新，赋能提升数据安全态势感知、风险研判等能力水平。加强第五代和第六代移动通信、工业互联网、物联网、车联网等领域的数据安全需求分析，推动专用数据安全技术产品创新研发、融合应用。支持数据安全产品云化改造，提升集约化、弹性化服务能力。

三、壮大数据安全服务

（七）推进规划咨询与建设运维服务。面向数据安全合规需求，发展合规风险把控、数据资产管理、安全体系设计等方面的规划咨询服务。围绕数据安全保护能力建设与运行需求，积极发展系统集成、监测预警、应急响应、安全审计等建设运维服务。面向数据有序开发利用的安全需求，发展数据权益保护、违约鉴定等中介服务。

（八）积极发展检测、评估、认证服务。建立数据安全检测评估体系，加强与网络安全等级保护评测等相关体系衔接，培育第三方检测、评估等服务机构，支持开展检测、评估人员的培训。支持开展数据安全技术、产品、服务和管理体系认证。鼓励检测、评估、认证机构跨行业跨领域发展，推动跨行业标准互通和结果互认。推动检测、评估等服务与数据安全相关标准体系的动态衔接。

四、推进标准体系建设

（九）加强数据安全产业重点标准供给。充分发挥标准对产业发展的支撑引领作用，促进产业技术、产品、服务和应用标准化。鼓励科研院所、企事业单位、普通高等院校及职业院校等各类主体积极参与数据安全产业评价、数据安全产品技术要求、数据安全产品评测、数据安全服务等标准制定。高质高效推进贯标工作，加大标准应用推广力度。积极参与数据安全国际标准组织活动，推动国内国际协同发展。

五、推广技术产品应用

（十）提升关键环节、重点领域应用水平。深度分析工业、电信、交通、金融、卫生健康、知识产权等领域数据安全需求，梳理典型应用场景，分类制定数据安全技术产品应用指南，促进数据处理各环节深度应用。推动先进适用数据安全技术产品在电子商务、远程医疗、在线教育、线上办公、直播新媒体等新型应用场景，

以及国家数据中心集群、国家算力枢纽节点等重大数据基础设施中的应用。推进安全多方计算、联邦学习、全同态加密等数据开发利用支撑技术的部署应用。

（十一）加强应用试点和示范推广。组织开展数据安全新技术、新产品应用试点，推进技术产品迭代升级，验证适用性和推广价值。遴选一批技术先进、特点突出、应用成效显著的数据安全典型案例和创新主体，加强示范引领。开展重点区域和行业数据安全应用示范，打造数据安全创新应用先进示范区，集中示范应用并推广数据安全技术产品和解决方案。

六、构建繁荣产业生态

（十二）推动产业集聚发展。立足数据安全政策基础、产业基础、发展基础等因素，布局建设国家数据安全产业园，推动企业、技术、资本、人才等加快向园区集中，逐步建立多点布局、以点带面、辐射全国的发展格局。鼓励地方结合产业基础和优势，围绕关键技术产品和重点领域应用，打造龙头企业引领、具有综合竞争力的高端化、特色化数据安全产业集群。

（十三）打造融通发展企业体系。实施数据安全优质企业培育工程，建立多层次、分阶段、递进式企业培育体系，发展一批具有生态引领力的龙头骨干企业，培育一批掌握核心技术、具有特色优势的数据安全专精特新中小企业、专精特新“小巨人”企业，培育一批技术、产品全球领先的单项冠军企业。发挥龙头骨干企业引领支撑作用，带动中小微企业补齐短板、壮大规模、创新模式，形成创新链、产业链优势互补，资金链、人才链资源共享的合作共赢关系。

（十四）强化基础设施建设。充分利用已有资源，建立健全数据安全风险库、行业分类分级规则库等资源库，支撑数据安全产品研发、技术手段建设，为数据安全场景应用测试等提供环境。建设数据安全产业公共服务平台，提供创新支持、供需对接、产融合作、能力评价、职业培训等服务，实现产业信息集中共享、供需两侧精准对接、公共服务敏捷响应。

七、强化人才供给保障

（十五）加强人才队伍建设。推动普通高等院校和职业院校加强数据安全相关学科专业建设，强化课程体系、师资队伍和实习实训等。制定颁布数据安全工程技术人员国家职业标准、实施数字技术工程师培育项目，培养壮大高水平数据安全工程师队伍，鼓励科研机构、普通高等院校、职业院校、优质企业和培训机构深化产教融合、协同育人，通过联合培养、共建实验室、创建实习实训基地、线上线下结合等方式，培养实用型、复合型数据安全专业技术技能人才和优秀管理人才。推进通过职业资格评价、职业技能等级认定、专项职业能力考核等，建立健全数据安全人才选拔、培养和激励机制，遴选推广一批产业发展急需、行业特色鲜明的数据安全优质培训项目。充分利用现有人才引进政策，引进海外优质人才与创新团队。

八、深化国际交流合作

（十六）推进国际产业交流合作。充分利用双多边机制，加强数据安全产业政策交流合作。加强与“一带一路”沿线国家数据安全产业合作，促进标准衔接和认证结果互认，推动产品、服务、技术、品牌“走出去”。鼓励国内外数据安全企业在技术创新、产品研发、应用推广等方面深化交流合作。探索打造数据安全产业国际创新合作基地。支持举办高层次数据安全国际论坛和展会。鼓励我国数据安全领域学者、企业家积极参与相关国际组织工作。

九、保障措施

（十七）加强组织领导。充分发挥国家数据安全工作协调机制作用，将发展数据安全产业作为提高数据安全保障能力的基础性任务，央地协同打造数据安全产业链创新链。各部门要加强统筹协调，形成发展合力，确保任务落实。各地有关部门要强化资源要素配置，推动产业发展重大政策、重点工程落地。

（十八）加大政策支持。研究利用财政、金融、土地等政策工具支持数据安全技术攻关、创新应用、标准研制和园区建设。支持符合条件的数据安全企业享受软件和集成电路企业、高新技术企业等优惠政策。引导各类金融机构和社会资本投向数据安全领域，支持数据安全保险服务发展。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。

（十九）优化发展环境。加快数据安全制度体系建设，细化明确政策要求。加强知识产权运用和保护，建立健全行业自律及监督机制，建立以技术实力、服务能力为导向的良性市场竞争环境。科学高效开展数据安全产业统计，健全产业风险监测机制，及时研判发展态势，处置突出风险，回应社会关切。加强教育引导，提升各类群体数据安全保护意识。

工业和信息化部

国家互联网信息办公室

国家发展和改革委员会

教育部

科学技术部

公安部

国家安全部

财政部

人力资源社会保障部

中国人民银行

国务院国有资产监督管理委员会

国家税务总局

国家市场监督管理总局

中国银行保险监督管理委员会

中国证券监督管理委员会

国家知识产权局

2023 年 1 月 3 日

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

《个人信息出境标准合同办法》已经 2023 年 2 月 3 日国家互联网信息办公室 2023 年第 2 次室务会议审议通过，现予公布，自 2023 年 6 月 1 日起施行。

国家互联网信息办公室主任　庄荣文

2023 年 2 月 22 日

个人信息出境标准合同办法

第一条 为了保护个人信息权益，规范个人信息出境活动，根据《中华人民共和国个人信息保护法》等法律法规，制定本办法。

第二条 个人信息处理者通过与境外接收方订立个人信息出境标准合同（以下简称标准合同）的方式向中华人民共和国境外提供个人信息，适用本办法。

第三条 通过订立标准合同的方式开展个人信息出境活动，应当坚持自主缔约与备案管理相结合、保护权益与防范风险相结合，保障个人信息跨境安全、自由流动。

第四条 个人信息处理者通过订立标准合同的方式向境外提供个人信息的，应当同时符合下列情形：

（一）非关键信息基础设施运营者；

（二）处理个人信息不满 100 万人的；

（三）自上年 1 月 1 日起累计向境外提供个人信息不满 10 万人的；

（四）自上年 1 月 1 日起累计向境外提供敏感个人信息不满 1 万人的。

法律、行政法规或者国家网信部门另有规定的，从其规定。

个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

第五条 个人信息处理者向境外提供个人信息前，应当开展个人信息保护影响评估，重点评估以下内容：

（一）个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；

（二）出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；

（三）境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；

（四）个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；

（五）境外接收方所在国家或者地区的个人信息保护政策和法规对标准合同履行的影响；

（六）其他可能影响个人信息出境安全的事项。

第六条 标准合同应当严格按照本办法附件订立。国家网信部门可以根据实际情况对附件进行调整。

个人信息处理者可以与境外接收方约定其他条款，但不得与标准合同相冲突。

标准合同生效后方可开展个人信息出境活动。

第七条 个人信息处理者应当在标准合同生效之日起 10 个工作日内向所在地省级网信部门备案。备案应当提交以下材料：

（一）标准合同；

（二）个人信息保护影响评估报告。

个人信息处理者应当对所备案材料的真实性负责。

第八条 在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评估，补充或者重新订立标准合同，并履行相应备案手续：

（一）向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；

（二）境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；

（三）可能影响个人信息权益的其他情形。

第九条 网信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、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供、非法使用。

第十条 任何组织和个人发现个人信息处理者违反本办法向境外提供个人信息的，可以向省级以上网信部门举报。

第十一条 省级以上网信部门发现个人信息出境活动存在较大风险或者发生个人信息安全事件的，可以依法对个人信息处理者进行约谈。个人信息处理者应当按照要求整改，消除隐患。

第十二条 违反本办法规定的，依据《中华人民共和国个人信息保护法》等法律法规处理；构成犯罪的，依法追究刑事责任。

第十三条 本办法自 2023 年 6 月 1 日起施行。本办法施行前已经开展的个人信息出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。

关于开展网络安全服务认证工作的实施意见

各省、自治区、直辖市和新疆生产建设兵团市场监管局（厅、委）、党委网信办、工业和信息化主管部门、公安厅（局），各省、自治区、直辖市通信管理局，各有关单位：

为推进网络安全服务认证体系建设，提升网络安全服务机构能力水平和服务质量，根据《网络安全法》《认证认可条例》，市场监管总局、中央网信办、工业和信息化部、公安部就开展国家统一推行的网络安全服务认证工作提出以下意见。

一、网络安全服务认证工作坚持“统一管理、共同实施、统一标准、规范有序”的基本原则。市场监管总局、中央网信办、工业和信息化部、公安部根据职责，加强认证工作的组织实施和监督管理，鼓励网络运营者等广泛采信网络安全服务认证结果，促进网络安全服务产业健康有序发展。

二、网络安全服务认证目录由市场监管总局会同中央网信办、工业和信息化部、公安部根据市场需求和产业发展状况确定并适时调整，现阶段包括检测评估、安全运维、安全咨询和等级保护测评等服务类别。认证规则和认证标志由市场监管总局征求中央网信办、工业和信息化部、公安部意见后另行制定发布。

三、市场监管总局、中央网信办、工业和信息化部、公安部联合组建由政府部门、科研机构、认证机构、标准化机构、网络安全服务机构和用户等相关方参与的网络安全服务认证技术委员会，协调解决认证体系建设和实施过程中出现的技术问题，研究提出认证目录、认证规则编写修订工作建议等。

四、从事网络安全服务认证活动的认证机构应当依法设立，符合《认证认可条例》《认证机构管理办法》规定的基本条件，具备从事网络安全服务认证活动的专业能力，并经市场监管总局根据各部门职责征求中央网信办、工业和信息化部、公安部意见后批准取得资质。

五、网络安全服务认证机构应当根据认证委托人提出的认证委托，按照网络安全服务认证基本规范、认证规则开展认证工作，建立可追溯工作机制对认证全过程完整记录。

六、网络安全服务认证机构应当公开认证收费标准和认证证书有效、暂停、注销或者撤销等状态，并按照有关规定报送网络安全服务认证实施情况及认证证书信息。

七、通过认证的网络安全服务机构应当按照有关法律法规、标准规范等开展网络安全服务工作，确保持续符合认证要求。

八、市场监管部门负责对网络安全服务认证机构、认证活动和认证结果进行监督管理，依法查处认证违法行为。

九、网信部门、工业和信息化部门、公安部门依据各自职责，推动认证结果采信应用，加强网络安全服务监督管理，促进网络安全服务产业发展，依法查处有关违法行为。

国家市场监督管理总局
中央网络安全和信息化委员会办公室
工业和信息化部
公安部
2023 年 3 月 15 日

关于调整网络安全专用产品安全管理有关事项的公告

2023年第1号

为加强网络安全专用产品安全管理，推动安全认证和安全检测结果互认，避免重复认证、检测，依据《中华人民共和国网络安全法》、《关于发布〈网络关键设备和网络安全专用产品目录（第一批）〉的公告》（2017 年第 1 号）、《国家认监委 工业和信息化部 公安部 国家互联网信息办公室关于发布承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）的公告》（2018 年第 12 号）、《关于统一发布网络关键设备和网络安全专用产品安全认证和安全检测结果的公告》（2022 年第 1 号），现将调整网络安全专用产品安全管理有关事项公告如下：

一、自 2023 年 7 月 1 日起，列入《网络关键设备和网络安全专用产品目录》的网络安全专用产品应当按照《信息安全技术 网络安全专用产品安全技术要求》等相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。

具备资格的机构是指列入《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》的机构。

国家互联网信息办公室、工业和信息化部、公安部、国家认证认可监督管理委员会发布更新《网络关键设备和网络安全专用产品目录》、《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录》。

二、自 2023 年 7 月 1 日起，停止颁发《计算机信息系统安全专用产品销售许可证》（简称销售许可证），产品生产者无需申领。此前已经获得销售许可证的产品在有效期内可继续销售或者提供。

三、自 2023 年 7 月 1 日起，停止执行《关于调整信息安全产品强制性认证实施要求的公告》（原国家质检总局、财政部、国家认证认可监督管理委员会 2009 年第 33 号）和《财政部 工业和信息化部 质检总局 认监委关于信息安全产品实施政府采购的通知》（财库〔2010〕48 号）。

四、国家互联网信息办公室会同工业和信息化部、公安部、国家认证认可监督管理委员会统一公布和更新符合要求的网络关键设备和网络安全专用产品清单，供社会查询和使用。

特此公告。
国家互联网信息办公室
工业和信息化部
公安部
财政部国家认证认可监督管理委员会
2023 年 4 月 12 日

网信部门行政执法程序规定

国家互联网信息办公室令

第 14 号《网信部门行政执法程序规定》已经 2023 年 2 月 3 日国家互联网信息办公室 2023 年第 2 次室务会议审议通过，现予公布，自 2023 年 6 月 1 日起施行。

国家互联网信息办公室主任　庄荣文

2023 年 3 月 18 日

网信部门行政执法程序规定

第一章　总则

第一条　为了规范和保障网信部门依法履行职责，保护公民、法人和其他组织的合法权益，维护国家安全和公共利益，根据《中华人民共和国行政处罚法》、《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、行政法规，制定本规定。

第二条　网信部门实施行政处罚等行政执法，适用本规定。

本规定所称网信部门，是指国家互联网信息办公室和地方互联网信息办公室。

第三条　网信部门实施行政执法，应当坚持处罚与教育相结合，做到事实清楚、证据确凿、依据准确、程序合法。

第四条 国家网信部门依法建立本系统的行政执法监督制度。

上级网信部门对下级网信部门实施的行政执法进行监督。

第五条 网信部门应当加强执法队伍和执法能力建设，建立健全执法人员培训、考试考核、资格管理和持证上岗制度。

第六条 网信部门及其执法人员对在执法过程中知悉的国家秘密、商业秘密或者个人隐私，应当依法予以保密。

第七条　执法人员与案件有直接利害关系或者有其他关系可能影响公正执法的，应当回避。

当事人认为执法人员与案件有直接利害关系或者有其他关系可能影响公正执法的，有权申请回避。

当事人提出回避申请的，网信部门应当依法审查，由网信部门负责人决定。决定作出之前，不停止调查。

第二章 管辖和适用

第八条　行政处罚由违法行为发生地的网信部门管辖。法律、行政法规、部门规章另有规定的，从其规定。

违法行为发生地包括违法行为人相关服务许可地或者备案地，主营业地、登记地，网站建立者、管理者、使用者所在地，网络接入地，服务器所在地，计算机等终端设备所在地等。

第九条　县级以上网信部门依职权管辖本行政区域内的行政处罚案件。法律、行政法规另有规定的，从其规定。

第十条　对当事人的同一个违法行为，两个以上网信部门都有管辖权的，由最先立案的网信部门管辖。

两个以上网信部门对管辖权有争议的，应当协商解决，协商不成的，报请共同的上一级网信部门指定管辖，也可以直接由共同的上一级网信部门指定管辖。

第十一条　上级网信部门认为必要的，可以直接办理下级网信部门管辖的案件，也可以将本部门管辖的案件交由下级网信部门办理。法律、行政法规、部门规章明确规定案件应当由上级网信部门管辖的，上级网信部门不得将案件交由下级网信部门管辖。

下级网信部门对其管辖的案件由于特殊原因不能行使管辖权的，可以报请上级网信部门管辖或者指定管辖。

设区的市级以下网信部门发现其所管辖的行政处罚案件涉及国家安全等情形的，应当及时报告上一级网信部门，必要时报请上一级网信部门管辖。

第十二条　网信部门发现受理的案件不属于其管辖的，应当及时移送有管辖权的网信部门。

受移送的网信部门应当将案件查处结果及时函告移送案件的网信部门；认为移送不当的，应当报请共同的上一级网信部门指定管辖，不得再次自行移送。

第十三条　上级网信部门接到管辖争议或者报请指定管辖的请示后，应当在十个工作日内作出指定管辖的决定，并书面通知下级网信部门。

第十四条　网信部门发现案件属于其他行政机关管辖的，应当依法移送有关行政机关。

网信部门发现违法行为涉嫌犯罪的，应当及时将案件移送司法机关。司法机关决定立案的，网信部门应当及时办结移交手续。

网信部门应当与司法机关加强协调配合，建立健全案件移送制度，加强证据材料移交、接收衔接，完善案件处理信息通报机制。

第十五条　网信部门对依法应当由原许可、批准的部门作出降低资质等级、吊销许可证件等行政处罚决定的，应当将取得的证据及相关材料送原许可、批准的部门，由其依法作出是否降低资质等级、吊销许可证件等决定。

第十六条　对当事人的同一个违法行为，不得给予两次以上罚款的行政处罚。同一个违法行为违反多个法律规范应当给予罚款处罚的，按照罚款数额高的规定处罚。

第三章　行政处罚程序

第一节　立案

第十七条　网信部门对下列事项应当及时调查处理，并填写案件来源登记表：

（一）在监督检查中发现案件线索的；

（二）自然人、法人或者其他组织投诉、申诉、举报的；

（三）上级网信部门交办或者下级网信部门报请查处的；

（四）有关机关移送的；

（五）经由其他方式、途径发现的。

第十八条　行政处罚立案应当符合下列条件：

（一）有涉嫌违反法律、行政法规和部门规章的行为，依法应当予以行政处罚；

（二）属于本部门管辖；

（三）在应当给予行政处罚的法定期限内。

符合立案条件的，应当填写立案审批表，连同相关材料，在七个工作日内报网信部门负责人批准立案，并指定两名以上执法人员为案件承办人。情况特殊的，可以延长至十五个工作日内立案。

对于不予立案的投诉、申诉、举报，应当将不予立案的相关情况作书面记录留存。

对于其他机关移送的案件，决定不予立案的，应当书面告知移送机关。　不予立案或者撤销立案的，承办人应当制作不予立案审批表或者撤销立案审批表，报网信部门负责人批准。

第二节　调查取证

第十九条　网信部门进行案件调查取证，应当由具有行政执法资格的执法人员实施。执法人员不得少于两人，并应当主动向当事人或者有关人员出示执法证件。必要时，可以聘请专业人员进行协助。

首次向案件当事人收集、调取证据的，应当告知其有申请执法人员回避的权利。

向有关单位、个人收集、调取证据时，应当告知其

有如实提供证据的义务。被调查对象和有关人员应当如实回答询问，协助和配合调查，及时提供依法应予保存的网络运营者发布的信息、用户发布的信息、日志信息等相关材料，不得阻挠、干扰案件的调查。

第二十条 网信部门在执法过程中确需有关机关或者其他行政区域网信部门协助调查取证的，应当出具协助调查函，协助调查函应当载明需要协助的具体事项、期限等内容。

收到协助调查函的网信部门对属于本部门职权范围的协助事项应当予以协助，在接到协助调查函之日起十五个工作日内完成相关工作；需要延期完成或者无法协助的，应当及时函告提出协助请求的网信部门。

第二十一条 执法人员应当依法收集与案件有关的证据，包括书证、物证、视听资料、电子数据、证人证言、当事人的陈述、鉴定意见、勘验笔录、现场笔录等。

电子数据是指案件发生过程中形成的，存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或者存储介质中，以数字化形式存储、处理、传输的，能够证明案件事实的数据。视听资料包括录音资料和影像资料。存储在电子介质中的录音资料和影像资料，适用电子数据的规定。

证据应当经查证属实，方可作为认定案件事实的根据。

以非法手段取得的证据，不得作为认定案件事实的根据。

第二十二条 立案前调查和监督检查过程中依法取得的证据材料，可以作为案件的证据使用。

对于移送的案件，移送机关依职权调查收集的证据材料，可以作为案件的证据使用。

第二十三条 网信部门在立案前，可以采取询问、勘验、检查、检测、检验、鉴定、调取相关材料等措施，不得限制调查对象的人身、财产权利。

网信部门立案后，可以对涉案物品、设施、场所采取先行登记保存等措施。

第二十四条 网信部门在执法过程中询问当事人或者其他有关人员，应当制作询问笔录，载明时间、地点、事实、经过等内容。询问笔录应当交询问对象或者其他有关人员核对确认，并由执法人员和询问对象或者其他有关人员签名。询问对象和其他有关人员拒绝签名或者无法签名的，应当注明原因。

第二十五条 网信部门对于涉及违法行为的场所、物品、网络应当进行勘验、检查，及时收集、固定书证、物证、视听资料和电子数据。

第二十六条 网信部门可以委托司法鉴定机构就案件中的专门性问题出具鉴定意见；不属于司法鉴定范围的，可以委托有能力或者有条件的机构出具检测报告或者检验报告。

第二十七条 网信部门可以向有关单位、个人调取能够证明案件事实的证据材料，并可以根据需要拍照、录像、复印和复制。

调取的书证、物证应当是原件、原物。调取原件、原物确有困难的，可以由提交证据的有关单位、个人在复制品上签字或者盖章，注明“此件由×××提供，经核对与原件（物）无异”的字样或者文字说明，注明出证日期、证据出处，并签名或者盖章。

调取的视听资料、电子数据应当是原始载体或者备份介质。调取原始载体或者备份介质确有困难的，可以收集复制件，并注明制作方法、制作时间、制作人等情况。调取声音资料的，应当附有该声音内容的文字记录。

第二十八条 在证据可能灭失或者以后难以取得的情况下，经网信部门负责人批准，执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存，制作登记保存物品清单，向当事人出具登记保存物品通知书。先行登记保存期间，当事人和其他有关人员不得损毁、销毁或者转移证据。 网信部门实施先行登记保存的，应当通知当事人或者持有人到场，并在现场笔录中对采取的相关措施情况予以记载。

第二十九条 网信部门对先行登记保存的证据，应当在七个工作日内作出以下处理决定：

（一）需要采取证据保全措施的，采取记录、复制、拍照、录像等证据保全措施后予以返还；

（二）需要检验、检测、鉴定的，送交具有相应资质的机构检验、检测、鉴定；

（三）违法事实不成立，或者先行登记保存的证据与违法事实不具有关联性的，解除先行登记保存。

逾期未作出处理决定的，应当解除先行登记保存。

违法事实成立，依法应当予以没收的，依照法定程序实施行政处罚。

第三十条 网信部门收集、保全电子数据，可以采取现场取证、远程取证和责令有关单位、个人固定和提交等措施。

现场取证、远程取证结束后，应当制作电子取证工作记录。

第三十一条 执法人员在调查取证过程中，应当要求当事人在笔录和其他相关材料上签字、捺指印、盖章或者以其他方式确认。

当事人拒绝到场，拒绝签字、捺指印、盖章或者以其他方式确认，或者无法找到当事人的，应当由两名执法人员在笔录或者其他材料上注明原因，并邀请其他有关人员作为见证人签字或者盖章，也可以采取录音、录像等方式记录。

第三十二条 对有证据证明是用于违法个人信息处理活动的设备、物品，可以采取查封或者扣押措施。

采取或者解除查封、扣押措施，应当向网信部门主要负责人书面报告并经批准。情况紧急，需要当场采取查封、扣押措施的，执法人员应当在二十四小时内向网信部门主要负责人报告，并补办批准手续。网信部门主要负责人认为不应当采取查封、扣押措施的，应当立即解除。

第三十三条 案件调查终结后，承办人认为违法事实成立，应当予以行政处罚的，撰写案件处理意见报告，草拟行政处罚建议书。

有下列情形之一的，承办人撰写案件处理意见报告，说明拟作处理的理由，报网信部门负责人批准后根据不同情况分别处理：

（一）认为违法事实不能成立，不予行政处罚的；

（二）违法行为情节轻微并及时改正，没有造成危害后果，不予行政处罚的；

（三）初次违法且危害后果轻微并及时改正，可以不予行政处罚的；

（四）当事人有证据足以证明没有主观过错，不予行政处罚的，法律、行政法规另有规定的，从其规定；

（五）案件不属于本部门管辖，应当移送其他行政机关管辖的；

（六）涉嫌犯罪，应当移送司法机关的。

第三十四条 网信部门在进行监督检查或者案件调查时，对已有证据证明违法事实成立的，应当责令当事人立即改正或者限期改正违法行为。

第三十五条 对事实清楚、当事人自愿认错认罚且对违法事实和法律适用没有异议的行政处罚案件，网信部门应当快速办理案件。

第三节 听证

第三十六条 网信部门作出下列行政处罚决定前，应当告知当事人有要求举行听证的权利。当事人要求听证的，应当在被告知后五个工作日内提出，网信部门应当组织听证。当事人逾期未要求听证的，视为放弃听证的权利：

（一）较大数额罚款；

（二）没收较大数额违法所得、没收较大价值非法财物；

（三）降低资质等级、吊销许可证件；

（四）责令停产停业、责令关闭、限制从业；

（五）其他较重的行政处罚；

（六）法律、行政法规、部门规章规定的其他情形。

第三十七条 网信部门应当在听证的七个工作日前，将听证通知书送达当事人，告知当事人及有关人员举行听证的时间、地点。

听证应当制作听证笔录，交当事人或者其代理人核对无误后签字或者盖章。当事人或者其代理人拒绝签字或者盖章的，由听证主持人在笔录中注明。

除涉及国家秘密、商业秘密或者个人隐私依法予以保密外，听证公开举行。

听证结束后，网信部门应当根据听证笔录，依照本规定第四十二条的规定，作出决定。第四节 行政处罚决定和送达

第三十八条 网信部门对当事人作出行政处罚决

定前，可以根据有关规定对其实施约谈，谈话结束后制作执法约谈笔录。

第三十九条 网信部门作出行政处罚决定前，应当填写行政处罚意见告知书，告知当事人拟作出的行政处罚内容及事实、理由、依据，并告知当事人依法享有的陈述、申辩等权利。

第四十条 当事人有权进行陈述和申辩。网信部门应当充分听取当事人的意见，对当事人提出的事实、理由和证据，应当进行复核；当事人提出的事实、理由或者证据成立的，网信部门应当采纳。

网信部门不得因当事人陈述、申辩而给予更重的处罚。

网信部门及其执法人员在作出行政处罚决定前，未依照本规定向当事人告知拟作出的行政处罚内容及事实、理由、依据，或者拒绝听取当事人的陈述、申辩，不得作出行政处罚决定，但当事人明确放弃陈述或者申辩权利的除外。

第四十一条 有下列情形之一，在网信部门负责人作出行政处罚的决定之前，应当由从事行政处罚决定法制审核的人员进行法制审核；未经法制审核或者审核未通过的，不得作出决定：

（一）涉及重大公共利益的；

（二）直接关系当事人或者第三人重大权益，经过听证程序的；

（三）案件情况疑难复杂、涉及多个法律关系的；

（四）法律、行政法规规定应当进行法制审核的其他情形。

法制审核由网信部门确定的负责法制审核的机构实施。网信部门中初次从事行政处罚决定法制审核的人员，应当通过国家统一法律职业资格考试取得法律职业资格。

（五）第四十二条 拟作出的行政处罚决定应当报网信部门负责人审查。网信部门负责人根据不同情况，分别作出如下决定：

（一）确有应受行政处罚的违法行为的，根据情节轻重及具体情况，作出行政处罚决定；

（二）违法行为轻微，依法可以不予行政处罚的，不予行政处罚；

（三）违法事实不能成立的，不予行政处罚；

（四）违法行为涉嫌犯罪的，移送司法机关。

第四十三条 对情节复杂或者重大违法行为给予行政处罚，网信部门负责人应当集体讨论决定。集体讨论决定的过程应当书面记录。

第四十四条 网信部门作出行政处罚决定，应当制作统一编号的行政处罚决定书。

行政处罚决定书应当载明下列事项：

（一）当事人的姓名或者名称、地址等基本情况；

（二）违反法律、行政法规、部门规章的事实和证据；

（三）行政处罚的种类和依据；

（四）行政处罚的履行方式和期限；

（五）申请行政复议、提起行政诉讼的途径和期限；

（六）作出行政处罚决定的网信部门名称和作出决定的日期。

行政处罚决定中涉及没收有关物品的，还应当附没收物品凭证。

行政处罚决定书必须盖有作出行政处罚决定的网信部门的印章。

第四十五条 网信部门应当自行政处罚案件立案之日起九十日内作出行政处罚决定。

因案情复杂等原因不能在规定期限内作出处理决定的，经本部门负责人批准，可以延长六十日。案情特别复杂或者情况特殊，经延期仍不能作出处理决定的，由上一级网信部门负责人决定是否继续延期，决定继续延期的，应当同时确定延长的合理期限；国家网信部门办理的行政处罚案件需要延期的，由本部门主要负责人批准。

案件处理过程中，听证、检测、检验、鉴定、行政协助等时间不计入本条第一款、第二款规定的期限。

第四十六条 行政处罚决定书应当在宣告后当场交付当事人；当事人不在场的，应当在七个工作日内依照《中华人民共和国民事诉讼法》的有关规定，将行政处罚决定书送达当事人。

当事人同意并签订确认书的，网信部门可以采用传真、电子邮件等方式，将行政处罚决定书等送达当事人。

第四章 执行和结案

第四十七条 行政处罚决定书送达后，当事人应当在行政处罚决定书载明的期限内予以履行。

当事人确有经济困难，可以提出延期或者分期缴纳罚款的申请，并提交书面材料。经案件承办人审核，确定延期或者分期缴纳罚款的期限和金额，报网信部门负责人批准后，可以暂缓或者分期缴纳。

第四十八条 网络运营者违反相关法律、行政法规、部门规章规定，需由电信主管部门关闭网站、吊销相关增值电信业务经营许可证或者取消备案的，转电信主管部门处理。

第四十九条 当事人对行政处罚决定不服，可以依法申请行政复议或者提起行政诉讼。

当事人对行政处罚决定不服，申请行政复议或者提起行政诉讼的，行政处罚不停止执行，法律另有规定的除外。

当事人申请行政复议或者提起行政诉讼的，加处罚款的数额在行政复议或者行政诉讼期间不予计算。

第五十条 当事人逾期不履行行政处罚决定的，作出行政处罚决定的网信部门可以采取下列措施：

（一）到期不缴纳罚款的，每日按罚款数额的百分之三加处罚款，加处罚款的数额不得超出罚款的数额；

（二）依照《中华人民共和国行政强制法》的规定申请人民法院强制执行。

网信部门批准延期、分期缴纳罚款的，申请人民法院强制执行的期限，自暂缓或者分期缴纳罚款期限结束之日起计算。

第五十一条 网信部门申请人民法院强制执行的，申请前应当填写履行行政处罚决定催告书，书面催告当事人履行义务，并告知履行义务的期限和方式、依法享有的陈述和申辩权；涉及加处罚款的，应当有明确的金额和给付方式。

当事人进行陈述、申辩的，网信部门应当对当事人提出的事实、理由和证据进行记录、复核，并制作陈述申辩笔录、陈述申辩复核意见书。当事人提出的事实、理由或者证据成立的，网信部门应当采纳。

履行行政处罚决定催告书送达十个工作日后，当事人仍未履行处罚决定的，网信部门可以填写行政处罚强制执行申请书，向所在地有管辖权的人民法院申请强制执行。

第五十二条 行政处罚决定履行或者执行后，有下列情形之一的，执法人员应当填写行政处罚结案报告，将有关案件材料进行整理装订，归档保存：

（一）行政处罚决定履行或者执行完毕的；

（二）人民法院裁定终结执行的；

（三）案件终止调查的；

（四）作出本规定第四十二条第二项至第四项决定的；

（五）其他应当予以结案的情形。

结案后，执法人员应当将案件材料按照档案管理的有关规定立卷归档。案卷归档应当一案一卷、材料齐全、规范有序。

第五十三条 网信部门应当依法以文字、音像等形式，对行政处罚的启动、调查取证、审核、决定、送达、执行等进行全过程记录，归档保存。

第五十四条 网信部门实施行政处罚应当接受社会监督。公民、法人或者其他组织对网信部门实施行政处罚的行为，有权申诉或者检举；网信部门应当认真审查，发现有错误的，应当主动改正。

第四章 附则

第五十五条 本规定中的期限以时、日计算，开始的时和日不计算在内。期限届满的最后一日是法定节假日的，以法定节假日后的第一日为届满的日期。但是，法律、行政法规另有规定的除外。

第五十六条 本规定中的“以上”、“以下”、“内”均包括本数、本级。

第五十七条 国家网信部门负责制定行政执法相关文书格式范本。各省、自治区、直辖市网信部门可以参照文书格式范本，制定本行政区域行政执法所适用的文书格式并自行印制。

第五十八条 本规定自 2023 年 6 月 1 日起施行。2017 年 5 月 2 日公布的《互联网信息内容管理行政执法程序规定》（国家互联网信息办公室令第 2 号）同时废止。

邮政局关于印发《寄递服务用户个人信息安全管理规定》和《邮政行业安全信息报告和处理规定》的通知

国邮发〔2014〕52号

各省、自治区、直辖市邮政管理局：

《寄递服务用户个人信息安全管理规定》和《邮政行业安全信息报告和处理规定》于2014年2月28日经国家邮政局2014年第4次局长办公会议审议通过，现印发给你们，请遵照执行。

邮 政 局

2014年3月19日

寄递服务用户个人信息安全管理规定

第一章 总 则

第一条 为加强邮政行业寄递服务用户个人信息安全管理，保护用户合法权益，维护邮政通信与信息安全，促进邮政行业健康发展，根据《中华人民共和国邮政法》、《全国人大常委会关于加强网络信息保护的规定》、《邮政行业安全监督管理办法》等法律、行政法规和有关规定，制定本规定。

第二条 在中华人民共和国境内经营和使用寄递服务涉及用户个人信息安全的活动以及相关监督管理工作，适用本规定。

第三条 本规定所称寄递服务用户个人信息（以下简称寄递用户信息），是指用户在使用寄递服务过程中的个人信息，包括寄（收）件人的姓名、地址、身份证件号码、电话号码、单位名称，以及寄递详情单号、时间、物品明细等内容。

第四条 寄递用户信息安全监督管理坚持安全第一、预防为主、综合治理的方针，保障用户个人信息安全。

第五条 国务院邮政管理部门负责全国邮政行业寄递用户信息安全监督管理工作。

省、自治区、直辖市邮政管理机构负责本行政区域内的邮政行业寄递用户信息安全监督管理工作。

按照国务院规定设立的省级以下邮政管理机构负责本辖区的邮政行业寄递用户信息安全监督管理工作。

国务院邮政管理部门和省、自治区、直辖市邮政管理机构以及省级以下邮政管理机构，统称为邮政管理部门。

第六条 邮政管理部门应当与有关部门相互配合，健全寄递用户信息安全保障机制，维护寄递用户信息安全。

第七条 邮政企业、快递企业及其从业人员应当遵守国家有关信息安全管理的规定及本规定，防止寄递用户信息泄露、丢失。

第二章 一般规定

第八条 邮政企业、快递企业应当建立健全寄递用户信息安全保障制度和措施，明确企业内部各部门、岗位的安全责任，加强寄递用户信息安全管理和安全责任考核。

第九条 以加盟方式经营快递业务企业应当在加盟协议中订立寄递用户信息安全保障条款，明确被加盟人与加盟人的安全责任。加盟人发生信息安全事故时，被加盟人应当依法承担相应安全管理责任。

第十条 邮政企业、快递企业应当与其从业人员签订寄递用户信息保密协议，明确保密义务和违约责任。

第十一条 邮政企业、快递企业应当组织从业人员进行寄递用户信息安全保护相关知识、技能培训，加强职业道德教育，不断提高从业人员的法制观念和责任意识。

第十二条 邮政企业、快递企业应当建立寄递用户信息安全投诉处理机制，公布有效联系方式，接受并及时处理有关投诉。

第十三条 邮政企业、快递企业受网络购物、电视购物和邮购等经营者委托提供寄递服务的，在与委托方签订协议时，应当订立寄递用户信息安全保障条款，明确信息使用范围和方式、信息交换安全保护措施、信息泄露责任划分等内容。

第十四条 邮政企业、快递企业委托第三方录入寄递用户信息的，应当确认其具有信息安全保障能力，并订立信息安全保障条款，明确责任划分。第三方发生信息安全事故导致寄递用户信息泄露、丢失的，邮政企业、快递企业应当依法承担相应责任。

第十五条 未经法律明确授权或者用户书面同意，邮政企业、快递企业及其从业人员不得将其掌握的寄递用户信息提供给任何单位或者个人。

第十六条 公安机关、国家安全机关或者检察机关的工作人员依照法律规定程序调阅、检查寄递详情单实物及电子信息档案，邮政企业、快递企业应当配合，并对有关情况予以保密。

第十七条 邮政企业、快递企业应当建立寄递用户信息安全应急处置机制。对于突发的寄递用户信息安全事故，应当立即采取补救措施，按照规定报告邮政管理部门，并配合邮政管理部门和相关部门的调查处理工作，不得迟报、漏报、谎报、瞒报。

第三章 寄递详情单实物信息安全管理

第十八条 邮政企业、快递企业应当加强寄递详情单管理，对空白寄递详情单发放情况进行登记，对号段进行全程跟踪，形成跟踪记录。

第十九条 邮政企业、快递企业应当加强营业场所、处理场所管理，严禁无关人员进出邮件（快件）处理、存放场地，严禁无关人员接触、翻阅邮件（快件），防止寄递详情单实物信息（以下简称实物信息）在处理过程中泄露。

第二十条 邮政企业、快递企业应当优化寄递处理流程，减少接触实物信息的处理环节和操作人员。

第二十一条 邮政企业、快递企业应当采用有效技术手段，防止实物信息在寄递过程中泄露。

第二十二条 邮政企业、快递企业应当配备符合国家标准的安全监控设备，安排具有专门技术和技能的人员，对收寄、分拣、运输、投递等环节的实物信息处理进行安全监控。

第二十三条 邮政企业、快递企业应当建立健全寄递详情单实物档案管理制度，实行集中封闭管理，确定集中存放地，及时回收寄递详情单妥善保管。设立、变更集中存放地，应当及时报告所在地邮政管理部门。

第二十四条 邮政企业、快递企业应当对寄递详情单实物档案集中存放地设专人管理，采取必要的安全防护措施，确保存储安全。

第二十五条 邮政企业、快递企业应当建立并严格执行寄递详情单实物档案查询管理制度。内部人员因工作需要查阅档案时，应当确保档案完整无损，并做好查阅登记，不得私自携带离开存放地。

第二十六条 寄递详情单实物档案应当按照国家

相关标准规定的期限保存。保存期满后，由企业进行集中销毁，做好销毁记录，严禁丢弃或者贩卖。

第二十七条 邮政企业、快递企业应当对实物信息安全保障情况进行定期自查，记录自查情况，及时消除自查中发现的信息安全隐患。

第四章 寄递详情单电子信息安全管理

第二十八条 邮政企业、快递企业应当按照国家规定，加强寄递服务用户信息相关信息系统和网络设施的安全管理。

第二十九条 邮政企业、快递企业信息系统的网络架构应当符合国家信息安全管理规定，合理划分安全区域，实现各安全区域之间有效隔离，并具有防范、监控和阻断来自内部和外部网络攻击破坏的能力。

第三十条 邮政企业、快递企业应当配备必要的防病毒软件、硬件，确保信息系统和网络具有防范计算机病毒的能力，防止恶意代码破坏信息系统和网络，避免信息泄露或者被篡改。

第三十一条 邮政企业、快递企业构建信息系统和网络，应当避免使用信息系统和网络供应商提供的默认密码、安全参数，并对通过开放公共网络传输的寄递用户信息采取加密措施，严格审查并监控对信息系统、网络设备的远程访问。

第三十二条 邮政企业、快递企业在采购计算机软件、硬件产品或者技术服务时，应当与供应商签订保密协议，明确其安全责任，以及在发生信息安全事件时配合邮政管理部门和相关部门调查的义务。

第三十三条 邮政企业、快递企业应当建立信息系统安全内部审计制度，定期开展内部审计，对发现的问题及时整改。

第三十四条 邮政企业、快递企业应当加强信息系统及网络的权限管理，基于权限最小化和权限分离原则，向从业人员分配满足工作需要的最小操作权限和可访问的最小信息范围。

邮政企业、快递企业应当加强对信息系统和数据库的管理，使网络管理人员仅具有进行信息系统、数据库、网络运行维护和优化的权限。网络管理人员的维护操作须经安全管理员授权，并受到安全审计员的监控和审计。

第三十五条 邮政企业、快递企业应当加强信息系统密码管理，使用高安全级别密码策略，定期更换密码，禁止将密码透露给无关人员。

第三十六条 邮政企业、快递企业应当加强寄递用户电子信息的存储安全管理，包括：

（一）使用独立物理区域存储寄递用户信息，禁止非授权人员进出该区域。

（二）采用加密方式存储寄递用户信息。

（三）确保安全使用、保管和处置存有寄递用户信息的计算机、移动设备和移动存储介质。明确管理数据存储设备、介质的负责人，建立设备、介质使用和借用登记制度，限制设备输出接口的使用。存储设备和介质报废的，应当及时删除其中的寄递用户信息数据，并销毁硬件。

第三十七条 邮政企业、快递企业应当加强寄递用户信息的应用安全管理，对所有批量导出、复制、销毁用户个人信息的操作进行审查，并采取防泄密措施，同时记录进行操作的人员、时间、地点和事项，留作信息安全审计依据。

第三十八条 邮政企业、快递企业应当加强对离岗人员的信息安全审计，及时删除或者禁用离岗人员系统账户。

第三十九条 邮政企业、快递企业应当制定本企业与市场相关主体的信息系统安全互联技术规则，对存储寄递服务信息的信息系统实行接入审查，定期进行安全风险评估。

第五章 监督管理

第四十条 邮政管理部门依法履行下列职责：

（一）制定保障寄递用户信息安全的政策、制度和相关标准，并监督实施；

（二）监督、指导邮政企业、快递企业落实信息安全责任制，督促企业加强寄递用户信息安全管理；

（三）对寄递用户信息安全进行监测、预警和应急管理；

（四）监督、指导邮政企业、快递企业开展寄递用户信息安全宣传教育和培训；

（五）依法对邮政企业、快递企业实施寄递用户信息安全监督检查；

（六）组织调查或者参与调查寄递用户信息安全事故，依法查处违反寄递用户信息安全管理规定的行为；

（七）法律、行政法规和规章规定的其他职责。

第四十一条 邮政管理部门应当加强邮政行业寄递用户信息安全管理制度和知识的宣传，强化邮政企业、快递企业及其从业人员的信息安全管理意识，提高用户对个人信息安全保护的认识。

第四十二条 邮政管理部门应当加强邮政行业寄递用户信息安全运行的监测预警，建立信息管理体系，收集、分析与信息安全有关的各类信息。

下级邮政管理部门应当及时向上一级邮政管理部门报告邮政行业寄递用户信息安全情况，并根据需要通报工业和信息化、通信管理、公安、国家安全、商务和工商行政管理等相关部门。

第四十三条 邮政管理部门应当对邮政企业、快递企业建立和执行寄递用户信息安全管理制度，规范从业人员信息安全保护行为，防范信息安全风险等情况进行检查。

第四十四条 邮政管理部门发现邮政企业、快递企业存在违反寄递用户信息安全管理规定，妨害或者可能妨害寄递用户信息安全的，应当依法进行调查处理。违法行为涉及其他部门管理职权的，邮政管理部门应当会同有关部门对涉案邮政企业、快递企业进行调查处理。

第四十五条 邮政管理部门应当加强对邮政企业、快递企业及其从业人员遵守本规定情况的监督检查。

第四十六条 邮政企业、快递企业拒不配合寄递用户信息安全监督检查的，依照《中华人民共和国邮政法》第七十七条的规定予以处罚。

第四十七条 邮政企业、快递企业及其从业人员因泄露寄递用户信息对用户造成损失的，应当依法予以赔偿。

第四十八条 邮政企业、快递企业及其从业人员违法提供寄递用户信息，尚未构成犯罪的，依照《中华人民共和国邮政法》第七十六条的规定予以处罚。构成犯罪的，移送司法机关追究刑事责任。

第四十九条 任何单位和个人有权向邮政管理部门举报违反本规定的行为。邮政管理部门接到举报后，应当依法及时处理。

第五十条 邮政管理部门可以在行业内通报邮政企业、快递企业违反寄递用户信息安全管理规定行为、信息安全事件，以及对有关责任人员进行处理的情况。必要时可以向社会公布上述信息，但涉及国家秘密、商业秘密和个人隐私的除外。

第五十一条 邮政管理部门及其工作人员对在履行职责过程中知悉的寄递用户信息应当保密，不得泄露、篡改或者损毁，不得出售或者非法向他人提供。

第五十二条 邮政管理部门工作人员在寄递用户信息安全监督管理工作中滥用职权、玩忽职守、徇私舞弊，依照《邮政行业安全监督管理办法》第五十五条的规定予以处理。

第六章 附 则

第五十三条 本规定自发布之日起施行。

邮政行业安全信息报告和处理规定

第一章 总 则

第一条 为规范邮政行业安全信息报告和处理工作，根据《中华人民共和国邮政法》、《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》、《生产安全事故报告和调查处理条例》、《邮政行业安全监督管理办法》等法律、行政法规和有关规定，制定本规定。

第二条 本规定所称应当报告和处理的安全信息，是指邮政行业突发事件信息和邮政企业、快递企业日常生产经营中与安全有关的运营信息。

邮政管理部门、邮政企业、快递企业报告和处理安全信息，适用本规定。

第三条 邮政行业安全信息报告和处理工作应当按照“渠道畅通、反应迅速、协调联动、科学有序”的工作要求，实现安全信息报告和处理的规范化。

第四条 安全信息的报告应当及时、准确和完整，任何单位和个人不得迟报、漏报、谎报或者瞒报；信息的处理应当遵循快速高效、协同配合、分级负责的原则。

第五条 邮政管理部门、邮政企业、快递企业应当完善安全信息报告和处理制度，畅通信息报送渠道，健全安全信息报告和处理工作体系，确保及时报告和处理有关安全信息。

邮政企业、快递企业应当确定专门机构和专门的安全信息员负责安全信息的收集、报告和处理工作。设立、变更安全信息员，应当第一时间报所在地省级以下邮政管理机构备案。

邮政管理部门应当指定人员负责安全信息的受理和报告工作，人员或者联系方式变更的，应当及时通报邮政企业、快递企业，并报告上级邮政管理部门。

第六条 邮政管理部门、邮政企业、快递企业应当加强安全信息报告和处理的宣传培训，增强有关人员的责任意识，提高安全信息报告和处理能力。

第七条 邮政管理部门应当收集、统计、分析与行业安全运行有关的信息，及时向邮政企业、快递企业发出安全预警。

邮政企业、快递企业应当加强日常生产经营的安全监测和信息分析，完善监测网络，明确监测项目，建立健全安全信息数据库，并按邮政管理部门要求报送安全信息。

第八条 安全信息应当以书面形式报告。以传真、电子邮件等方式报出信息后，应当进行电话确认。

情况紧急时，应当先用电话等方式快报，随后补报书面材料。

第二章 安全信息类别

第九条 本规定所称邮政行业突发事件信息是指《国家邮政业突发事件应急预案》（以下简称邮政业应急预案）列举的事件信息，主要包括：

（一）因气象灾害、地震灾害、地质灾害、生物灾害和森林草原火灾等自然灾害，造成或者可能造成人员伤亡，大量邮件或者快件积压、丢失、损毁，其他财产损失，信息系统瘫痪，企业生产经营中断或者寄递服务阻断；

（二）因各类有毒害性化学品泄漏、环境污染和生态破坏等事故灾难，造成或者可能造成人员伤亡，大量邮件或者快件积压、丢失、损毁，其他财产损失，信息系统瘫痪，企业生产经营中断或者寄递服务阻断；

（三）因传染病疫情、群体性不明原因疾病、食品安全、职业危害和动物疫情等公共卫生事件，造成或者可能造成人员伤亡，大量邮件或者快件积压、丢失、损毁，其他财产损失，信息系统瘫痪，企业生产经营中断或者寄递服务阻断；

（四）因恐怖袭击事件、民族宗教事件、经济安全事件、涉外突发事件和群体性事件造成或者可能造成人员伤亡，大量邮件或者快件积压、丢失、损毁，其他财产损失，信息系统瘫痪，企业生产经营中断或者寄递服务阻断；

（五）因企业不正当竞争、经营权纠纷、兼并重组、破产倒闭等行业安全风险，以及火灾等生产安全事故、设施和设备故障、交通运输事故，造成或者可能造成人员伤亡，大量邮件或者快件积压，财产损失，企业生产经营中断或者寄递服务阻断；

（六）其他对寄递渠道安全畅通构成威胁、造成影响的突发事件信息。

第十条 本规定所称邮政企业、快递企业日常生产经营中与安全有关的运营信息（以下简称日常安全信息）主要包括：

（一）寄递过程中发现枪支弹药、毒品、非法出版物等禁寄物品；

（二）用户使用寄递服务的信息遭非法泄露；

（三）邮件、快件被盗窃、非法扣留、冒领、私自开拆、隐匿、毁弃，或者运送邮件、快件的车辆被非法拦截、强登、扒乘；

（四）邮政企业、快递企业负责人或者安全管理人员变更；

（五）邮政企业、快递企业主要负责人因违法行为被有关部门立案调查；

（六）邮政企业、快递企业因违反安全监管规定或者因其他违法行为被有关部门查处；

（七）邮政企业、快递企业因安全管理工作成效突出受到有关部门表彰；

（八）邮政企业、快递企业发现重大安全隐患自身难以排除；

（九）其他日常生产经营中与安全有关的重要运营信息。

第十一条 邮政企业、快递企业应当对日常安全信息进行分析、判断，发生或者可能发生突发事件的，按照突发事件信息报告处理。

第三章 突发事件信息的报告和处理

第十二条 国家邮政业突发事件应急工作办公室（以下简称国家邮政业应急办公室）负责全国邮政行业特别重大突发事件（Ⅰ级）信息的接收、报告和处理，以及日常接警值班工作；国务院邮政管理部门值班室同时承担信息的接收工作。

省、自治区、直辖市邮政管理机构和省级以下邮政管理机构负责本辖区邮政行业突发事件信息的接收、报告和处理工作。

第十三条 邮政企业、快递企业和邮政管理部门应当实行特殊时期 24 小时值班制度，接收、核实、报告、跟踪有关突发事件信息，并按照职责权限承担或者参与事件的处置。

第十四条 邮政企业、快递企业发生突发事件，符合下列情形之一的，应当在 1 小时内向突发事件发生地的省级以下邮政管理机构报告，并视情况依法向公安、国家安全、海关、交通运输、安全生产监督管理等相关部门报告：

（一）本企业人员死亡或者失踪 1 人以上，或者重伤 3 人以上；

（二）邮件、快件 1 次丢失、损毁 100 件以上，或者积压 1000 件以上；

（三）邮件、快件、现金、车辆、邮资凭证等财物经济损失严重；

（四）邮寄爆炸物、生物病原体、生物毒素、有毒害性化学品、放射性物品等，在寄递过程中发生爆炸、泄漏；

（五）邮件处理中心、快件分拨中心内发生重大事

故，生产经营中断；

（六）邮政企业、快递企业生产经营场所遭到围堵，导致生产经营中断或者寄递服务阻断；

（七）其他可能严重影响寄递渠道畅通的情形。

第十五条 邮政企业、快递企业发生突发事件，属于本规定第十四条所列情形之外的，应当在 2 小时内向突发事件发生地的省级以下邮政管理机构报告，并视情况依法向公安、国家安全、海关、交通运输、安全生产监督管理等相关部门报告。

第十六条 邮政企业、快递企业依照邮政业应急预案，对可能构成重大突发事件（Ⅱ级）的，可以直接向所在地省、自治区、直辖市邮政管理机构报告，对可能构成特别重大突发事件（Ⅰ级）的，可以直接向国务院邮政管理部门报告。

第十七条 报告突发事件信息，应当包括下列内容：

（一）报告单位的名称、地址及联系人、联系方式等基本情况；

（二）信息来源以及事件发生时间、地点、起因、性质和基本过程；

（三）已经造成或者可能造成的伤亡人数（包括失踪、涉险的人数）、邮件或者快件的损失情况、生产经营中断或者寄递服务阻断情况以及初步估计的直接经济损失；

（四）已经采取的措施和可能发展的趋势；

（五）其他应当报告的情况。

使用电话等方式快报，应当包括下列内容：

（一）报告单位的名称、地址及联系人、联系方式；

（二）信息来源以及事件发生时间、地点；

（三）已经造成或者可能造成的损失情况。

第十八条 突发事件具体情况暂时不清楚的，负责报告的单位可以先报概况，随后补报全面情况。

突发事件信息报告后出现新情况的，负责报告的单位应当及时续报。

第十九条 突发事件发生地省级以下邮政管理机构接到突发事件信息报告后，应当尽快开展研判。依照邮政业应急预案，对可能构成特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）的，应当在 1 小时内报告省、自治区、直辖市邮政管理机构；对可能构成较大突发事件（Ⅲ级）的，应当在 2 小时内报告省、自治区、直辖市邮政管理机构。

第二十条 省、自治区、直辖市邮政管理机构接到突发事件信息报告后，应当尽快组织研判，依照邮政业应急预案，对可能构成特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）的，应当在 1 小时内报告国务院邮政管理部门。

第二十一条 国家邮政业应急办公室接到突发事

件信息报告后，应当立即组织研判，依照邮政业应急预案，对可能构成特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）的，应当迅速按照规定程序报分管局领导。分管局领导认为构成特别重大突发事件（Ⅰ级）的，应当在 1 小时内报国家邮政业应急领导小组。

国务院邮政管理部门值班室接到突发事件信息报告后，应当第一时间转交国家邮政业应急办公室。

第二十二条 国家邮政业应急领导小组经研判确定构成特别重大突发事件（Ⅰ级）的，应当立即报告国务院和交通运输部，并通报国务院有关部门。向国务院报告特别重大突发事件（Ⅰ级）的时间，自突发事件发生最迟不得超过 4 小时。

报国务院的“值班信息”通过国务院政府信息网报送；报交通运输部及通报相关部门的“值班信息”应当采取传真或者电子邮件等方式。

第二十三条 邮政管理部门、邮政企业、快递企业在报告和处理突发事件的同时，应当依照应急预案立即开展应急处置工作。

第二十四条 国家邮政业应急办公室负责组织特别重大突发事件（Ⅰ级）的应急处置工作；每日至少向国家邮政业应急领导小组报告 1 次处置工作情况。重要信息及时续报国务院和交通运输部。

省、自治区、直辖市邮政管理机构负责重大突发事件（Ⅱ级）的应急处置工作，每日至少向国家邮政业应急办公室报告一次处置工作情况。

省级以下邮政管理机构负责较大突发事件（Ⅲ级）和一般突发事件（Ⅳ级）的应急处置工作，应当及时向省、自治区、直辖市邮政管理机构报告处置工作情况。

第二十五条 国家邮政业应急领导小组对邮政行业突发事件处置工作作出指示或者批示的，国家邮政业应急办公室应当及时向有关单位传达。

第二十六条 负责突发事件处置工作的邮政管理部门应当在突发事件发生之日起 60 日内，将有关工作总结报告上一级邮政管理部门。

国家邮政业应急办公室将工作总结报告国家邮政业应急领导小组，并按照应急领导小组的要求报交通运输部。

第二十七条 邮政行业预警启动和应急响应信息的报告和处理依照邮政业应急预案执行。

第四章 日常安全信息的报告和处理

第二十八条 对下列安全信息，邮政企业、快递企业应当在第一时间报告所在地省级以下邮政管理机构，并视情况依法报告当地公安、安全生产监督管理等部门：

（一）寄递过程中发现枪支弹药、毒品、非法出版物等禁寄物品；

（二）用户使用寄递服务的信息遭非法泄露；

（三）邮件、快件被盗窃、非法扣留、冒领、私自开拆、隐匿、毁弃，情况严重；

（四）运送邮件、快件的车辆被非法拦截、强登、扒乘，情况严重；

（五）发现重大安全隐患。

第二十九条 省级以下邮政管理机构接到本规定第二十八条所列信息报告后，应当立即核实有关情况，并与公安、安全生产监督管理等部门共同做好处置工作。对存在下列情形之一的，应当在收到信息报告后 2 小时内报省、自治区、直辖市邮政管理机构：

（一）寄递过程中发现枪支弹药、易燃易爆品等危及公共安全的禁寄物品；

（二）用户使用寄递服务的信息遭非法泄露 500 条以上；

（三）邮件、快件被盗窃、非法扣留 100 件以上，或者邮件、快件被冒领、私自开拆、隐匿、毁弃 50 件以上；

（四）运送邮件、快件的车辆被非法拦截、强登、扒乘 2 辆以上；

（五）重大安全隐患没有及时排除。

第三十条 省、自治区、直辖市邮政管理机构接到本规定第二十九条所列信息报告后，应当指导安全信息涉及的省级以下邮政管理机构做好处置工作，并于处置工作结束后将有关情况报告国务院邮政管理部门。

对于事关重大并且确实超出省、自治区、直辖市邮政管理机构处理能力的，应当及时报告国务院邮政

管理部门。

第三十一条 国务院邮政管理部门接到省、自治区、直辖市邮政管理机构信息报告后，应当协调公安、安全生产监督管理等部门妥善处理。

第三十二条 有下列情形之一的，邮政企业、快递企业应当在情形发生之日起 3 日内，向所在地省级以下邮政管理机构报告：

（一）邮政企业、快递企业负责人或者安全管理人员变更；

（二）邮政企业、快递企业主要负责人被有关部门立案调查；

（三）邮政企业、快递企业因违反安全监管规定或者因其他违法行为被有关部门查处。

第三十三条 邮政管理部门接到本规定第三十二条所列信息报告后，应当对有关情况进行核查；事关重大，可能影响行业稳定的，应当及时上报。

第三十四条 邮政企业、快递企业应当分类汇总本单位安全信息，报告所在地省级以下邮政管理机构，于每年 7 月 10 日前报送半年汇总表，于每年 1 月 10 日前报送上一年的年度汇总表。

第三十五条 省级以下邮政管理机构应当分类汇总本辖区安全信息，报告省、自治区、直辖市邮政管理机构，于每年 7 月 15 日前报送半年汇总表，于每年 1 月 15 日前报送上一年的年度汇总表。

省、自治区、直辖市邮政管理机构应当分类汇总本辖区安全信息，报告国务院邮政管理部门，于每年 7 月 25 日前报送半年汇总表，于每年 1 月 25 日前报送上一年的年度汇总表。

必要时，上级邮政管理部门可以要求下级邮政管理部门随时报告安全信息。

第五章 监督检查

第三十六条 邮政管理部门应当利用消费者申诉热线、媒体报道、市场检查、企业报告等多种手段和渠道，获取行业安全信息并及时处理。

第三十七条 邮政管理部门应当依法对邮政企业、快递企业建立健全安全信息报告和处理制度、安全预警监测、应急救援、从业人员安全教育培训等相关情况进行监督检查。

第三十八条 邮政管理部门应当对安全信息报告和处理工作中作出突出贡献的单位和个人给予表彰、奖励。

第三十九条 邮政管理部门应当定期向全行业通报监督检查情况；对检查发现的问题，及时约谈有关单位和人员，责令其整改，监督其落实。

对涉及公共安全和广大用户合法权益的安全信息，应当依照有关规定适时向社会公布。

第四十条 邮政企业、快递企业未按本规定报告和处理安全信息的，邮政管理部门应当依照《邮政行业安全监督管理办法》第五十条的规定予以处罚。

第四十一条 邮政管理部门未按规定及时报告处理行业安全信息的，上级邮政管理部门应当责令改正，可以给予通报，并可以对有关责任人员给予行政处分。

第四十二条 有关单位和人员迟报、漏报、谎报、瞒报事故的，依照《中华人民共和国安全生产法》、《生产安全事故报告和调查处理条例》相关规定处理。

第六章 附 则

第四十三条 本规定所称的迟报、漏报、谎报和瞒报，依照下列情形认定：

（一）报告安全信息、事件或者事故的时间超过规定时限的，属于迟报；

（二）因过失对应当上报的安全信息、事件或者事故发生的时间、地点、类别、伤亡人数、直接经济损失等内容遗漏未报的，属于漏报；

（三）故意不如实报告事件或者事故发生的时间、地点、类别、伤亡人数、直接经济损失等有关内容的，属于谎报；

（四）故意隐瞒已经发生的事件或者事故，经有关部门查证属实的，属于瞒报。

第四十四条 本规定有关数量的规定中，所称“以上”包括本数，“以下”不包括本数；关于日期的规定均为自然日。

第四十五条 本规定自发布之日起施行。

武汉市网络安全应急技术支撑单位拟入选单位公示

根据市委网信办和市公安局联合印发的《关于开展武汉市网络安全应急技术支撑单位遴选工作的通知》（武网办发〔2022〕8 号），经单位自主申报、形式审查、实战评价和专家评审，拟遴选 30 家单位为武汉市网络安全应急技术支撑单位，有效期 2 年。现将拟入选单位名单予以公示。

公示时间：2023 年 1 月 18 日 -2023 年 1 月 24 日

联 系 人：王量　杨希

联系电话：16602793119　13807182527

武汉市委网信办

武汉市公安局

2023 年 1 月 18 日

武汉市网络安全应急技术支撑单位拟入选单位名单（排名不分先后）

1、北京天融信网络安全技术有限公司
2、杭州安恒信息技术股份有限公司
3、武汉安域信息安全技术有限公司
4、北京神州绿盟科技有限公司
5、亚信科技（成都）有限公司
6、三六零数字安全科技集团有限公司
7、武汉华康科技有限公司
8、湖北东方网盾信息安全技术有限公司
9、武汉安天信息技术有限责任公司
10、武汉市德发电子信息有限责任公司
11、奇安信网神信息技术(北京)股份有限公司
12、武汉烽火信息集成技术有限公司
13、武汉云视科技技术有限公司
14、深圳海云安网络安全技术有限公司
15、武汉吧哒科技股份有限公司
16、武汉易通科技有限公司
17、湖北中网科技有限公司
18、湖北珞格科技发展有限公司
19、智网安云（武汉）信息技术有限公司
20、鸣飞伟业技术有限公司
21、北京长亭科技有限公司
22、杭州迪普科技股份有限公司
23、曙光网络科技有限公司
24、北京山石网科信息技术有限公司
25、武汉安经纬业信息安全技术有限公司
26、光谷技术有限公司
27、恒安嘉新（北京）科技股份公司
28、湖北省网络信息安全技术管控中心
29、湖北省电子信息产品质量监督检验院
30、武汉网信联盾网络安全技术中心

中共武汉市网络安全协会支部正式成立并揭牌

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，协会已于 2023 年 2 月 21 日正式成立党支部，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，铭记庄严的承诺，牢记共产党员的政治责任、工作担当和光荣使命，自觉增强四个意识，坚定党员对党的事业奋斗终身的决心和愿望，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，精诚团结、攻坚克难，努力向党组织交上一份满意的答卷。

会议同时邀请了主管部门相关处室负责同志宣读《关于同意成立中共武汉市网络安全协会支部的批复》文件，并与武汉市互联网行业党委委员聂益军同志，共同为协会党支部揭牌。

支部全体党员集体学习了习近平总书记在二十次党代会上的报告，传达学习了第十四届全国人民代表大会第一次会议和中国人民政治协商会议第十四届全国委员会第一次会议精神。

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组织迈进的步伐。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。

我会党建工作得到省市网信主管部门支持和关注

近日，武汉市网络安全协会党支部召开党员大会，并举行了党支部成立揭牌仪式。

武汉市网络安全协会是在武汉市委网信办主管下，由武汉地区从事网络安全行业龙头企业、安全服务机构，以及高等院校、企事业单位组成的非营利社会组织。自 2018 年成立以来，协会积极作为、勇于探索，不断拓展服务职能，上线全国首个移动应用安全公益检测平台，参与行业标准制定，开展会员互访交流、网络安全知识公益行及讲座等活动，在增强网络安全意识，提高网络安全防护技能，营造安全、文明、健康、和谐的网络环境作出了积极贡献。

下一步，武汉市网络安全协会党支部将加强自身建设、发挥特色优势、积极创新实践，激发协会会员企业党组织和党员生机活力，发挥连接政府、促进企业发展、团结党员和群众的纽带作用。（武汉市委网信办 供稿）

https://hbcac.gov.cn/gzdt/202303/t20230322_6559.shtml

党日活动
“红心互联铸网盾，蓝海扬帆助安恒”
党建主题顺利开展

为积极贯彻习近平总书记关于加强新经济组织、新社会组织、新就业群体党的建设的重要指使精神，响应国家“两新”工作有关规定和要求，“以党建促发展”不断加强网络安全企业和社会组织党的政治建设工作，引领企业和社会组织健康发展，4 月 12 日，中共武汉安恒信息科技有限公司支部、中共武汉市网络安全协会支部联合开展“红心互联铸网盾，蓝海扬帆助安恒”党建主题活动，并举行了中共武汉安恒信息科技有限公司支部揭牌仪式。

双方党支部参观了安恒公司展厅及党建工作专栏，深入交流党建工作心得，共同认为应在行业及企业内全面加强党的组织建设，创新支部管理模式，做好各项服务工作，提升社会影响力。

本次活动还特别邀请了武汉市委网信办、汉阳区委相关领导莅临指导，并传达了党的二十大会议关于网信工作的重要精神。

光明网专访我会会长潘宣辰
——从换道超车到国民引擎！
潘宣辰：“我很自豪让技术融入产业”

网络强国这十年——行业回顾篇

随着移动互联网快速发展和全面覆盖，移动安全威胁发生重大迁移：一方面，不良应用行为、欺诈诱导营销、用户欺瞒及隐私窃取等侵害用户权益的风险应用出现新一轮扩张；另一方面，移动互联网野蛮生长导致生态出现无序竞争局面，风险应用依附于移动互联网业务，正通过更加多样化的方式侵害用户权益，成为用户安全及权益新痛点，给整个产业的治理带来新的难题。

在我国移动安全行业发展版图上，安天移动安全通过将反病毒技术领先优势融入互联网产业，用“关口前移”的方式为超过 30 亿终端用户织密了移动应用风险防护网，也为主管部门提供了“良赢治理”方案和感知处置能力。

近日，安天科技集团执行总裁、武汉市网络安全协会会长潘宣辰，做客光明网“网络强国这十年”专栏，畅谈投身移动安全创业故事及行业发展的观察与思考。

投身移动安全创业，选择站在同一起跑线上的新赛道

2005 年前后，85 后青年潘宣辰还在武汉大学信息安全专业就读，这是国内第一个信息安全本科专业。在

武汉安域周佑源：成为最信赖的网络安全服务商

一次演讲授课上，潘宣辰结识了当时在武汉大学做兼职教授的网安前辈安天创始人肖新光（Seak）。

当时，我国在 PC 安全时代的核心技术还处于一个追赶的姿态。Seak 给学生时代的潘宣辰渲染了一副宏大的国家安全及民族软件创新产业格局，并提出希望能找到一个新的技术领域或在一个新的操作系统平台上，可以由国内相关的研发团队自主去实现基础核心技术的突破和创新。

这个目标打动了潘宣辰。毕业后，在安天的支持下，他选择了移动安全方向创业发展。潘宣辰认为，PC 时代几乎所有的技术，包括产品和商业模式在引入到移动场景后，都得到了进一步的叠加演进。结合移动特有的产业及生态结构，在移动安全方向上，必然会形成不一样的产业及生态安全需求，也同样会产生新的技术定义以及商业模式。

“得益于移动互联网的蓬勃发展，我们在这个全新的领域，和国内其他优秀厂商以及海外厂商相比，站在一个起跑线上，而且相比之下，安天以往在 PC 端积累的技术视野，在全新的领域进行技术架构和商业模式创新时，没有太多的历史包袱，又具有科班出身的发展优势。”潘宣辰说。

自主研发反病毒引擎，打破欧美安全厂商十余年独大

2010 年以前，PC 时代国内比较领先的安全厂商在海外的排行榜上并不是很靠前，最高排名第 8 位，多数徘徊在第 10 名左右。有了这个先例，潘宣辰和团队最开始设定目标是移动安全领域能够进入到世界前 8 位。

当时，团队初期的技术实力在移动领域优势并不明显。潘宣辰坦言，像海外的卡巴斯基、比特梵德，以及国内的瑞星、金山、360、腾讯等，其实都已经关注到，移动安全必然是未来一大趋势，当时大家都在积极投入技术研发。

深蹲之后，才能更好的起跳。最初，由于技术理念上有较大的差异，团队的优势并不明显。在和国内外厂商交流之后，才发现这是技术理念上的差异造成的。

比如，友商更多的是直接把 PC 时代的经验快速复制到移动时代，而安天是以本地检测算法引擎以及基于机器学习的专家智能分析工程平台运营体系为主，所以“工程化”传统较重，成果的形成需要较长时间的积累。

2013 年前后，安天的优势开始凸显。当时，国际知名安全软件评测机构 AV-Test 的移动安全首次测评中，安天 AVL 移动反病毒引擎的检出率指标平均领先行业水平 10% 以上。这是国内安全厂商第一次在世界范围的反病毒领域呈现出技术压倒性优势，也就在那年，安天移动安全打破了欧美厂商的垄断，以 100% 的检出率成为首个获得 AV-Test“移动年度最佳奖项”的亚洲厂商。

技术的真正价值，需要用市场和产业的方式来“回答”

在 2014 年取得核心技术突破的时候，他们也有卖掉团队的机会。潘宣辰和团队在“财务诱惑”和“产业挑战”之间，选择了后者。

潘宣辰认为，技术本身并没有常胜将军，也并不见得会永远占据优势。“这项技术到底是不是真的有价值，最终还需要用市场和产业的方式来回答。如果不去真正进入市场、进入产业的话，我自己觉得会特别后悔。因为这样就等于止步于技术了。”潘宣辰说。

安天移动安全在 2015 年开始探索商业化路径，选择了关口前移的产业融入线路。即通过选择与手机厂商广泛合作，通过操作系统级的嵌入式来进行技术落地，并且在这个基础上去构建新的商业模式。从 2015 年至今，安天威胁检测引擎为全球超过三十亿部智能终端设备提供了操作系统内置的安全检测能力。

“在移动安全的核心技术领域上，我们目前仍然保持着世界前列的水准。在检测这个技术点上，我们应该一直是第一第二的位置。”潘宣辰说。

（来源：光明网 监制：张宁 采访：李政葳 拍摄/后期：刘昊 李飞 配音：雷渺鑫 [责编：孔繁鑫]）

原文标题：【网络强国这十年】从换道超车到国民引擎！安天科技潘宣辰：“很自豪让技术融入产业”

原文链接：https://share.gmw.cn/wlaq/2022-10/25/content_36113748.htm

他从北京回来武汉创业，深耕网络安全领域，犹如弄潮儿一般搏击风浪，带领着企业发展壮大，获得湖北省专精特新小巨人企业、高新技术企业、武汉市科技小巨人企业、国家网络安全基地瞪羚企业等荣誉。

今天让我们近距离了解轮值会长—武汉安域信息安全技术有限公司（以下简称"武汉安域"）总经理周佑源。

选择一条正确的赛道

1983 年，周佑源出生于人才辈出的湖北黄冈，他始终坚信知识是成长的动力，为此他积极学习，最终考入合肥工业大学，后又成功考取北京交通大学硕士学位。

2007 年夏天，恰逢上海安言信息技术有限公司在北京有个项目，需要招募信息安全方面的人才，正在北京交通大学读研二的周佑源凭借着扎实的技术实力，顺利通过面试，加入安言咨询的项目。就这样，周佑源一头扎进了网络信息安全领域，从此便在这个行业一路前行，一直到现在。

2007 年 12 月，周佑源加入了北京信息安全测评中心（以下简称"北京测评中心"），一干就是三年。他说："在北京测评中心的三年时间里，做事规范、守原则是我收获的最宝贵的财富。"而这样的工作作风也一直伴随着周佑源，直到现在。

从安言咨询到北京测评中心、百度再到易宝支付，每一个阶段都给周佑源带来了全新的体验。而正是这些宝贵的从业经历，为他后来为武汉安域创业史打下了坚实的基础。

他乡纵有当头月，不及家乡一盏灯；落叶总要归根，再远也要有归程。同时，随着网络安全信息的重要性不断提升，网安行业已呈现需求爆发之势，并逐步辐射中部地区。在此背景下，周佑源毅然决定携家眷踏上了千里回乡之路。回到武汉，他遇到了事业上的合伙人、人生的知己叶全军。周佑源和叶全军以梦为马、凝聚共识，决定筹划在湖北成立一家等保测评机构，聚焦于为政府、企业、教育、医疗等行业提供等保测评等安全咨询服务。之前的从业经历给他带来了别人无比羡慕的优势：既了解等保机构运作，又了解甲方企业的安全需求，同时还拥有扎实的技术实力。

2014 年上半年，武汉安域迎来了第一个转折点——成功获取等级保护测评机构的资质，正式成为一家以等保测评业务为主的企业。

如今，武汉安域已是湖北省委网信办、湖北省公安厅、武汉市委网信办、武汉市公安局及其他省市主管单位重要技术支撑单位，为电子政务、能源、医疗、教育、交通、水利、金融、公共通信和信息服务等重要行业和领域提供专业的网络安全服务。

创新驱动，稳中求变谋发展

在网安发展的大浪潮下，中部地区网安市场有了长足的发展。随着企业等保要求逐渐普及，越来越多的企业开始重视安全建设。而日益频发的网络安全事件，如勒索病毒、信息泄露、网页篡改等，进一步让企业认识到安全的重要性。

凭借着扎实的服务和高效率的项目交付，武汉安域在业界的口碑越来越响亮。而后，武汉安域不断优化企业安全服务方案，并以行业类别进行划分，为不同行业的用户提供更贴合其业务属性的安全服务，成为行业的领头羊。

2016 年 9 月，中央网信办批复武汉市设立国家网络安全人才与创新基地，打造国内首个"网络安全学院 + 创新产业谷"。

2017 年 9 月，公司将注册地迁入位于武汉临空港的国家网安基地，由此开启了"加速跑"发展模式。

2017 年至 2018 年，连续两年成为湖北省市场占有率的 NO.1；

2019 年，军运会期间武汉安域参与核心赛事系统和 53 个场馆的等级测评与安全保障工作。

2020 年疫情时期，武汉安域作为省网信部门和网安部门技术支撑单位，积极参与全省健康码安全测试、省重点医疗机构日常安全保障、邮件安全隐患排查和"清明网上祭扫"专项保障工作等多项技术支撑工作，为湖北省抗疫期间的网络工作提供可靠的安全保障，勇于承担企业责任和社会责任，不畏疫情，全力保障主管部门网络安全。

2020 年至今，武汉安域持续斥资近 2000 万元在国家网安基地打造网络安全综合性攻防实验室和行业技术应用场景，用于支撑网络对抗、技能竞赛、实战化人才培养、职业技能认定、行业技术成果展示、安全研究和试点示范等工作。

2021 年 6 月，武汉安域总部乔迁新址，正式安家于武汉市洪山区正堂时代 28 楼。

2022 年武汉安域成功入选为湖北省专精特新“小巨人”企业。

2020 年至今，武汉安域从测评机构向专业安全服务机构转变，并被国家网络安全基地授予瞪羚企业荣誉。

如今，武汉安域由最初的 7 人创业团队发展壮大成为一支 150 余人的网络安全服务商，并且是湖北省内资质最全、单项级别最高的专业安全服务机构，获得中国网络安全审查技术与认证中心颁发的信息安全应急处理（一级）、风险评估、安全运维服务资质；工

业信息安全产业发展联盟颁发的工业信息安全应急服务支撑单位；国家计算机网络应急技术处理协调中心颁发的网络安全应急服务支撑单位（省级）；中国合格评定国家认可委员会颁发的 CNAS 实验室认可证书和 CNAS 检验机构认可证书；湖北省市场监督管理局颁发的 CMA 检验检测机构资质认定证书。

近十年来，武汉安域砥砺前行、不忘初心，靠着勇往直前的拼搏精神，战胜了创业路上一个又一个的艰难险阻。累计服务客户 2000+，获得专业认可 20 余项，支撑认可 50 余项，累计获得用户感谢信 100+，收获了各级主管部门的一致认可和表彰。

周佑源说：“成为最信赖的网络安全服务商是武汉全体安域人的奋斗愿景。在监管部门、主管部门的指导下，以行业专家资源为基础，联同优秀的咨询规划、系统集成、云服务商、网络安全设备厂家等形成网络安全综合防控体系服务商，为行业用户提供更专业、全

方位的安全支撑工作，为助力国家网络安全建设而持续奋进。”

同时，他提到：“品牌影响力不是策划出来的，而是以责任为骨、以专业为板、以创新为帆、以共赢为桨，以百里风趟的姿态，乘长风破万里浪，在暴风雨中浇筑出来的。”

2021 年 7 月，湖北省委常委、政法委书记肖菊华一行莅临国家网安基地考察调研，并对武汉安域在国家网安基地的落户和贡献给予了充分肯定，特别是对武汉安域为第七届世界军人运动会、建党 100 周年等重大活动提供网络安全保障给予了高度评价。

2021 年 9 月，中央宣传部副部长，中央网信办主任、国家网信办主任庄荣文莅临国家网安基地考察调研。庄荣文强调要着力培育网络安全良性生态，加快推进国家网络安全人才与创新基地建设，建立完善网络安全技术创新体系，加强网络安全产业统筹规划和整体布局，探索走出一条网络安全教育、技术、产业融合发展之路。

作为湖北武汉地区专业的网络安全企业，武汉安域积极投身各项社会公益和行业自律工作，2020 年被推选为武汉市网络安全协会副会长单位，与协会各成员单位一起参与和支持协会各项工作：积极投入社会公益工作，筹建培训中心，开展网络安全专题培训；参与武汉市重要时期网络安全应急支撑保障工作；参与推动协会团标工作，并经理事会同意成为 2023 年第一期轮值会长单位继续深度参与协会工作。

周佑源表示：“非常荣幸成为武汉市网安协会的第一期轮值会长单位，我们将坚持在武汉市委网信办的指导下，推动协会各项内部工作建设。武汉安域将秉承严于律己、厚德守正的初心，着力促进网络安全行业自律。时刻牢记服务宗旨，服务好会员及会员单位。继续完善协会的专家智库，充分发挥科技工作者和技术骨干赋能国家、社会、行业网信发展的能力。同时，积极开展武汉市网络安全人才培养教育工作，为社会输送更多的实用型人才。

武汉市网络安全协会 2023 年第一次会长办公会顺利召开

2023 年 1 月 10 日，武汉市网络安全协会 2023 年第一次会长办公会在协会汉口办公室顺利召开。协会会长单位武汉安天信息技术有限责任公司，副会长单位武汉烽火信息集成技术有限公司、曙光网络科技有限公司、武汉安域信息安全技术有限公司、中国联合网络通信有限公司武汉市分公司、深圳海云安网络安全技术有限公司湖北分公司、湖北珞格科技发展公司、武汉吧哒科技股份有限公司等单位负责人及代表出席，理事单位神州绿盟武汉科技有限公司、会员单位武汉华康科技有限公司、武汉安恒信息技术有限公司、亚信安全武汉分公司等单位代表列席本次会议。会议由协会秘书长刘悦恒主持。

会议集体学习了党的二十大精神，专题分享了党的二十大关于网信工作的重要论述。

会议认为，党的二十大是在全党全国各族人民迈上全面建设社会主义现代化国家新征程、向第二个百年奋斗目标进军的关键时刻召开的一次十分重要的大会。协会对党的二十大精神实质和核心要义进行再学习、再领会，持续推动学习宣传贯彻党的二十大精神不断走深走实。同时，要把学习宣传党的二十大精神与推动武汉网络安全事业发展结合起来，围绕党的二十大对网络强国建设作出的部署要求，在市委网信办的指导关心下，认真研究谋划 2023 年的工作，推动协会新的一年取得新更大成效。

会议听取了秘书处起草的《协会 2022 年工作总结》（讨论稿）和《协会 2022 年度财务报告》（草案）。

会议认为，在武汉市委网信办的指导关心下，在各位会长、副会长（单位）的领导下，在广大会员的支持下，在秘书处全体同事的努力下，2022 年协会各项工作稳步推进、活动开展亮点突出、日常工作务实饱满、服务能力显著提升，财务状况不断改善，会长副会长单位对今年以来的各项工作一致认可，建议材料进一步优化细节总结不足。

会议集体研究讨论了《协会 2023 年工作要点》（讨论稿）。

会议认为，2023 年将是全面贯彻落实党的二十大精神的开局之年，协会应紧密围绕武汉网信工作重点，谋篇布局开拓创新，做好各项支撑服务工作。

会议还集体研究讨论了《协会 2023 年团体标准工作规划》，研究《武汉市网络安全应急技术支撑单位自律公约》（讨论稿），《武汉市网络安全协会轮值会长工作制度》（讨论稿），研究筹建协会二级机构的必要性和可行性、确定二级机构名称、工作任务、筹备组成员、筹备程序、基本工作制度等事项。

会议要求，各项工作要认真组织精心谋划，会长、副会长、秘书长作为协会主要负责人应共同带头，加大投入，深入协会各项工作，为武汉网安事业发展贡献力量。

会议听取了秘书处作的《关于成立协会党支部工作进展的说明》。

会议指出，应积极落实中共中央办公厅《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，按照主管部门要求，我会作为网络安全专业性社会团体，应尽快成立党的组织。加强协会党建是巩固和扩大党的执政基础的需要，也是是促进社会组织健康发展的根本保证。

会议还研究了协会其他工作事项。

会议决定，本次会长办公会研究成果应提交理事会或会员大会决议。农历春节过后应尽快召开协会第二届第二次理事会或会员大会。

我会受到主管部门市委网信办感谢表扬

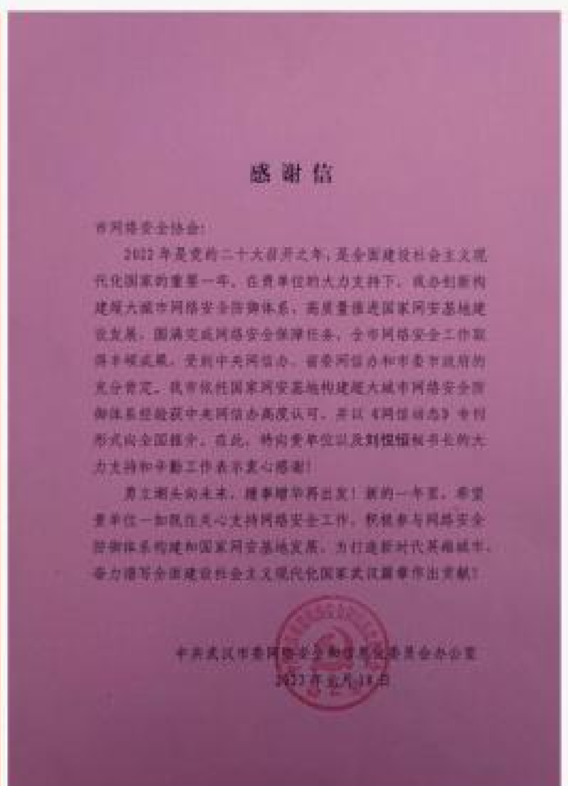
2022 年是党的二十大召开之年，也是实施“十四五”规划、全面建设社会主义现代化国家的重要一年。武汉市网络安全协会在武汉市委网信办的指导关心下，在协会理事会的领导下，在广大会员的支持下，坚持用全局视野和长远眼光，谋划推进武汉网络安全事业高质量发展，各项工作开创了新局面、取得了新成效，得到了广大会员单位和主管部门的认可。

近日，我会受到协会主管单位—市委网信办的表扬与感谢，我会上下深感荣幸，倍感责任重大。

2023 年协会将紧紧围绕我市网信中心工作，做好各项支撑服务，与广大会员单位一起，一如既往地发挥各自优势，支持武汉社会经济发展，共同推动我市网络安全工作迈上新台阶。


感谢信

武汉市网络安全协会：


感谢信

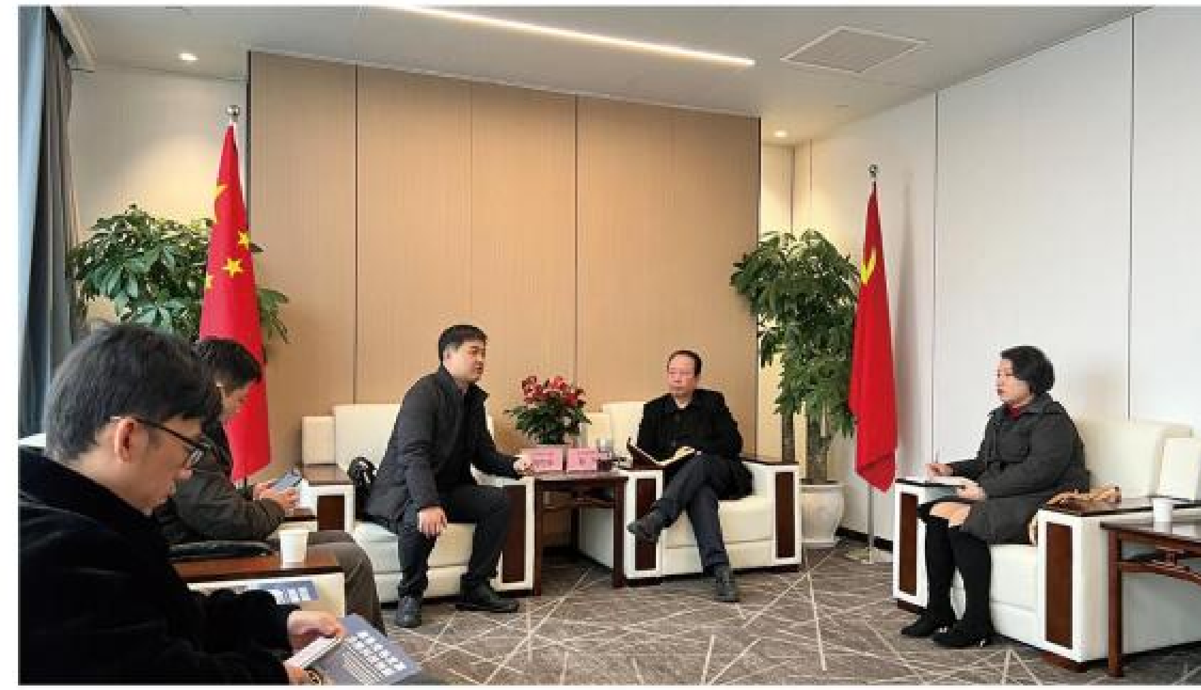
市网络安全协会：

2022 年是党的二十大召开之年，是全面建设社会主义现代化国家的重要一年。在贵单位的大力支持下，我办创新构建超大城市网络安全防御体系，高质量推进国家网安基地建设发展，圆满完成网络安全保障任务，全市网络安全工作取得丰硕成果，受到中央网信办、省委网信办和市委市政府的充分肯定。我市依托国家网安基地构建超大城市网络安全防御体系经验获中央网信办高度认可，并以《网信动态》专刊形式向全国推介。在此，特向贵单位以及刘悦恒秘书长的大力支持和辛勤工作表示衷心感谢！

勇立潮头向未来，踔事增华再出发！新的一年里，希望贵单位一如既往关心支持网络安全工作，积极参与网络安全防御体系构建和国家网安基地发展，为打造新时代英雄城市、奋力谱写全面建设社会主义现代化国家武汉篇章作出贡献！

中共武汉市委网络安全和信息化委员会办公室

我会赴武汉东湖高新科技保险发展促进中心开展工作交流



2 月 9 日，武汉市网络安全协会秘书长刘悦恒、政企服务部主任乔奇、公共关系发展部主任严媛、网络安全保险工作委员会（筹）周韬一行应邀赴武汉东湖高新科技保险发展促进中心拜访交流。武汉东湖高新科技保险发展促进中心主任孙智等领导予以热情接待。

孙智主任首先代表东湖科保对协会的来访表示热烈欢迎，并向大家介绍了东湖科保的基本情况，并带领参观企业展厅。网安协会刘秘书长感谢东湖科保的热情接待，并介绍了协会的职能和发展规划。

双方就共同推动我市网络安全、金融服务创新融合发展、培养网络安全保险新业态、促进网络安全产业高质量发展等方面进行深入探讨。双方今后将深入开展相关合作，共同为武汉网络安全科技发展做出贡献。

第七届“烽火杯”创新创业大赛总决赛成功举办

2月22日，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，武汉国际创客中心、网安创新谷承办，武汉市网络安全协会、武汉大学、武汉科技大学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。烽火创新谷副总经理朱晓春致欢迎辞。

武汉大学国家网络安全学院教授吴黎兵、武汉科技大学教授胡威、与时投资董事长赵团结、清科创业武汉城市负责人王建、武汉抓现货科技董事长彭承路、武汉虹捷信息科技董事长管和鹏6位专家评委、以及来自企业和高校的12个总决赛项目团队成员、媒体机构等近百人参加了当日活动。

大赛自启动以来受到了政府机构、各知名高校、社会团体鼎力支持和认可。大赛历经项目征集、项目遴选、预赛、半决赛等赛程、在总决赛中，来自武汉威思众信息科技的基于终端零信任的APT攻击检测系统项目斩获大赛企业区一等奖，来自武汉大学国家网络安全学院的基于国密的智能网联车安全系统等项目斩获高校区金奖。大赛共计颁发了30余万的创新创业奖金，用以激励获奖团队。

本次大赛旨在通过赛事提高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、合作和资源共享的平台，支持创业者发展和企业做大做强。

我会政企服务部主任乔奇出席本次活动。

我会赴上海开展工作交流

为加强沪汉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。2月21日，武汉市网络安全协会秘书长刘悦恒、公共关系发展部主任严媛、网络安全保险工作委员会（筹）周韬一行赴上海市信息安全行业协会拜访交流。上海市信息安全行业协会秘书长王强、副秘书长代淑杰等协会负责人予以热情接待。

王秘书长对我会来访表示热烈欢迎，并详细介绍了上海协会在支撑主管部门、服务会员单位方面的工作经验。刘秘书长代表武汉协会对上海协会的接待表示感谢，介绍了武汉协会和武汉网络安全产业基本情况，对上海协会服务企业、规范行业、发展产业方面勇于实践，敢于探索的工作经验和优秀成果表示倾佩。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。

我会还应邀考察了上海协会副会长单位，我会会员单位—上海观安信息技术股份有限公司。观安信息是一家提供大数据+泛安全产品与服务的高新技术企业，公司聚焦数据安全、网络空间安全、5G安全、人工智能安全、工业互联网安全及公共安全等核心方向，为运营商、政府、金融、电力、公安、医疗等行业用户提供全面的信息安全解决方案。观安在武汉设立了研发基地。观安战略规划部总经理蒋韬等有关负责人参与接待。

本次赴上海开展工作交流，是我会为落实我市《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》《2023年武汉市科技创新工作要点》等文件精神，大力培育网络安全创新产业集群，努力搭建兄弟省市间产业交流合作平台的一项重要工作。后续我会将积极落实深化双方交流成果，不断扩大武汉网络安全产业朋友圈，为我市网络安全事业健康快速发展贡献力量！

工业和信息化部人才交流中心武汉办严功望主任来访我会

2023 年 3 月 2 日，工业和信息化部人才交流中心武汉办事处严功望主任一行到访我会秘书处座谈交流。武汉市网络安全协会秘书长刘悦恒、公共关系发展部主任严媛等热情接待，双方围绕工信部人才中心与协会工作的协同与合作事宜进行座谈交流。

座谈会上，严功望主任介绍了工信部人才交流中心以及武汉办事处的业务情况，希望双方充分发挥资源优势，强强联合，在网安人才体系建设、高层次人才培育以及创新平台运营等领域进行深入合作。

刘秘书长对严主任一行表示热烈欢迎，对工信部人才交流中心长期以来对我市网安人才培养工作的重视和支持表示感谢，介绍了协会近年来在主管部门服务支撑、会员服务、实战化网络安全人才培养、团体标准的规划与建设等重点工作，今年以来协会调研走访了十余所高等院校和网安企业，深入了解了目前我市网络安全专业产教融合、人才培养的状况，并将相关情况交换了意见。

刘秘书长表示，今后将积极落实深化双方交流成果，扎实推进我市网络安全实战化人才培养工作。

工业和信息化部人才交流中心是中央机构编制委员会办公室批准成立、国家事业单位登记管理局登记、工业和信息化部直属的公益二类事业单位，是工业和信息化部从事人才培养、人才交流、国际合作、智力引进、人力资源服务、人才领域研究咨询等方面工作的机构，承载着国家专业技术人才继续教育基地、国家中小企业公共服务示范平台、工业和信息化人才公共服务平台、工业和信息化部专业技术人才知识更新工程协调小组办公室、工业和信息化部企业经营管理人才素质提升工程协调小组办公室、工业和信息化部引进国外智力工作办公室等多重职能。中心坚持“打造工业和信息化领域国际化、专业化的权威人才服务机构”为发展定位，以“为制造强国和网络强国建设提供人才服务支撑”为使命。

武汉市网络安全协会第二届理事会第二次会议顺利召开

2023 年 3 月 3 日，武汉市网络安全协会第二届理事会第二次会议在武汉会议中心顺利召开。本次大会 27 名协会理事单位和监事代表参与了会议。会议由协会秘书长刘悦恒主持。武汉市委网信办网络安全处、国家网络安全人才与创新基地办公室有关负责人到场指导。

协会会长潘宣辰视频致欢迎辞，武汉市委网信办网络安全处、国家网络安全人才与创新基地办公室有关负责人致辞。

安天信息代表李迎雪宣读关于武汉市网络安全协会党支部成立的有关说明。经上级党组织批复，协会已于 2023 年 2 月 21 日正式成立党支部，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。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组织迈进的步伐。党支部成立后协会将开展以“党日”为主题的系列活动，以党组织建设为基础推进协会各项事业健康有序发展。

会议审议了《武汉市网络安全协会 2023 年第一批申请加入理事会单位名单》。会议表决通过湖北天融信网络安全技术有限公司、神州绿盟武汉科技有限公司新增为副会长单位；武汉新时通信息技术有限公司、武汉安恒信息科技有限公司、武汉华康科技有限公司、湖北东方网盾信息安全技术有限公司、奇安信安全技术（武汉）有限公司、亚信科技（成都）有限公司、武汉同德兴信息技术有限公司、杭州迪普科技股份有限公司新晋为理事单位。主管部门和协会领导向新晋单位代表进行了授牌并颁发了证书。

协会秘书处向大会作 2022 年工作总结报告和财务报告。报告指出，2022 年是党的二十大召开之年，也是实施“十四五”规划、全面建设社会主义现代化国家的重要一年。武汉市网络安全协会在武汉市委网信办的指导关心下，在各位会长、副会长（单位）的领导下，在广大会员的支持下，坚持用全局视野和长远眼光，谋划推进武汉网络安全事业高质量发展，各项工作开创了新局面、取得了新成效。

去年以来，协会积极开展会员互访交流活动，增强协会凝聚力；建设协会宣传平台持续扩大影响力；发动会员积极申报网络安全领域武汉英才评选；上线全国首个面向移动开发者的公益免费检测平台；不断推进团体标准化工作助推行业高质量发展；与在汉高校联合建立网络安全“专精特新”产业学院；积极发展会员深入会员服务会员，支持会员和行业开展形式多样的宣传活动；深入开展网络安全实战化人才培养工作，取得了一定成果。

大力举办各项活动，持续扩大武汉网络安全品牌影响力。去年，协会成功举办武汉市网络安全公益行“武汉云”大讲堂暨市直机关大讲堂活动；举办网络安全知识讲座走进武汉各服务业集聚区；承办 2022 年武汉市国家网络安全宣传周互动系列活动；协助市经信局协办武汉企业网络安全培训行业行系列活动；与长江日报联合举办“数创未来 • 安全护航”——武汉高校信息化建设与网络安全研讨会；协办 2022 中国 5G+ 工业互联网大会“5G+ 工业互联网安全分论坛”等多项网络安全大型活动。

协会主动当好主管部门助手参谋，圆满完成交办任务——协助主管部门推选了一批高水平网络安全专家队伍；承接多项课题研究；积极协助主管部门组织武汉网络安全应急支撑单位遴选、网络安全实战演练等多项工作，得到了主管部门表扬和感谢。

大会全票通过了《武汉市网安全协会 2022 年工作总结》、《武汉市网络安全协会 2023 年团体标准工作规划》、《武汉市网络安全应急技术支撑单位自律公约》、《武汉市网络安全协会轮值会长工作制度》及协会内部有关制度及二级机构筹备方案等工作制度和文件。与会代表认真履职，围绕我市网络安全实战化人才培养、智能汽车网络安全、网络安全保险、校园网络安全建设、团体标准研制等议题展开热烈讨论。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二次会议圆满结束。

武汉市网络安全协会第二届理事会第二次会议

2023 年“安域杯”网络安全技能大赛成功举办

2023 年 3 月 8 日，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，武汉艾迪时代网络技术有限公司、武汉菲奥达物联科技有限公司协办的—2023 年“安域杯”网络安全技能大赛成功举办。

大赛聚焦网络安全的攻防对抗特点，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。大赛邀请了 8 所院校、共 35 名选手。在比赛期间，高手妙招频频出现，选手们很快进入白热化抢分环节，积分交替上升，大赛赛况精彩纷呈，扣人心弦。选手们纷纷表示，参加本次比赛，除了要熟练掌握网络安全专业知识外，还要重视专业知识整合、快速反应能力、团队协作能力，学员们在本次大赛中共同磨砺成长，是一次很好的综合训练和实战机会，通过参加比赛不仅可以证明自己的能力，也为集体和企业争夺了荣誉。

附获奖名单：

冠军：彭诗雨　湖北警官学院 信息安全专业

亚军：熊　懿　湖北警官学院 网络安全与执法专业

季军：董雨桐　湖北警官学院 信息安全专业

优秀奖：

冯　卓　湖北警官学院 计算机科学与技术专业

陈立飞　湖北警官学院 信息安全专业

王任驰　武汉东湖学院 网络空间安全专业

凌宗业　湖北生物科技职业学院 信息安全管理技术应用专业

罗德康　武汉城市职业学院 计算机网络专业

武汉市网络安全协会与武汉东湖科技保险发展促进中心签订战略合作协议

三月春暖，樱花盛开，美丽武汉，生意盎然。

由武汉市网络安全协会主办的 2023 网络安全产业融合创新发展峰会“金融科技安全发展论坛”3 月 30 日在武汉举行。

本次论坛中，武汉市网络安全协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，共建东湖网络安全保险服务中心，共同开展网络风险管理研究和网络安全保险服务，为东湖和全市各类型单位提供网络安全保障。该中心将设在东湖高新区科技大厦武汉东湖科技保险发展促进中心内。

随着国家数字经济的快速发展，网络安全在国家安全中的地位日益凸显，习近平总书记指出：“没有网络安全就没有国家安全，网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。”去年底，工信部会同银保监会起草了《关于促进网络安全保险规范健康发展的意见（征求意见稿）》，文中指出，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，已日益成为转移、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。

武汉这座英雄之城，是中央网信办授予的全国唯一拥有“国家网络安全人才与创新基地”的国家中心城市，同时，武汉东湖高新区也是中国银保监会、湖北省人民政府批设的全国首个科技保险创新示范区。作为我市两大行业的代表机构，武汉市网络安全协会与武汉东湖科技保险发展促进中心的深入合作，是贯彻习近平总书记关于不断做强做优做大我国数字经济的重要讲话精神，落实《网络安全法》《数据安全法》《个人信息保护法》等国家法规的创新探索，也是响应各级主管部门要求的具体行动和国家赋予武汉的光荣使命。

双方共建的全国首家网络安全保险服务中心，将结合各自优势，通过技术合作、资源共享等方式，共同为服务对象提供“量身定制”的系统性网络安全保险服务，包括快速获取投保企业数字资产网络安全风险状况、快速评估被保企业网络安全风险敞口、自动化生成被保企业数字资产网络安全风险报告、持续监控被保企业网络安全状况、网络安全宣传、风险损失的经济补偿等服务。中心还将深入开展各项工作，制定系列网络安全保险服务流程、规范和标准，创新并推出更多服务和产品，共同构建“安全 + 保险 + 科技”的网络安全保险服务体系。

后续，双方将持续推动网络安全产业和保险服务融合创新，为国家网络安全人才与创新基地及武汉东湖科技保险创新示范区建设添砖加瓦，为全市数字经济高质量发展保驾护航，努力为全国网络安全和科技保险融合创新发展探索出新的模式。

2023 网络安全产业融合创新发展峰会 金融科技安全发展论坛成功举办

数字经济时代，金融科技飞速发展，包括大数据、云计算、生物识别、区块链、知识图谱等新兴技术与金融行业各项工作及业务开展深度融合，让金融行业工作呈现智能化、数字化和移动化的发展趋势，也让金融服务更加快捷、智能、普惠、利民，但相应的网络安全面临的挑战也更加复杂、严峻。

3月30日，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。

本次金融科技安全发展论坛特邀主管部门武汉市委网信办相关领导，主办方武汉市网络安全协会和承办方天融信科技集团负责人，金融行业代表武汉东湖科技保险发展促进中心、国任财产保险股份有限公司、武汉众邦银行股份有限公司相关负责人，还邀请了重点高校武汉大学信息管理学院、中南财经政法大学金融科技研究院等专家领导发表主题演讲，共议金融科技安全融合发展。

武汉市网络安全协会秘书长刘悦恒在致辞中表示，在新一轮科技革命和产业变革的背景下，金融科技蓬勃发展，人工智能、大数据、云计算、物联网等信息技术与金融业务深度融合，为金融发展提供源源不断的创新活力；金融科技蓬勃发展带来机遇的同时也带来了新的挑战，因此引导金融科技向善发展成为金融科技良性可持续发展的必答题。他倡议，金融科技安全发展需要各方面共同参与、深度协作，并呼吁各界携手，努力将网络安全产业和金融服务业融合发展的创新工作，推向新的台阶。

天融信科技集团高级副总裁江建平在致辞中表示，近年来，国家层面对于网络安全建设工作更加体系化，陆续出台了相关的法律法规及政策文件。金融行业，人民银行制定了《金融科技发展规划（2022-2025年）》，描绘了金融科技发展的宏伟蓝图，也提出了金融网络安全工作目标和重点任务，为金融机构落实网络安全工作提供了具体的行动指南。江建平指出，天融信科技集团作为“金融科技安全发展论坛”承办单位，深耕网络安全行业二十七年，始终以提升自主创新能力与核心竞争力为目标，不断为金融行业客户及合作伙伴提供专业的产品、服务及解决方案。希望通过此次论坛，团结业界各领域朋友，共同拓展金融行业网络安全市场，为行业安全发展做出贡献，实现互惠共赢！

中南财经政法大学金融科技研究院执行院长徐晟发表了以《金融科技与金融安全助力金融高质量发展》为主题的演讲，演讲围绕着新发展理念下金融高质量发展的五大原则、金融科技赋能金融业高质量发展、金融安全守护金融业高质量发展展开介绍。徐晟指出，金融科技有助于提升金融的普惠性和韧性，也能进一步赋能实体经济高质量发展，全面提升金融业数字化水平和综合实力。

武汉众邦银行股份有限公司金融科技管理部总经理田骏发表了以《互联网银行网络安全创新实践》为主题的演讲，演讲围绕着互联网银行网络安全面临的风险与挑战以及网络安全实践两大方面进行介绍。田总着重从安全架构整体规划、闭环的互联网资产管理流程体系、有效互联网资产监控架构、互联网资产管理实践、漏洞闭环管理、漏洞生命周期流程、漏洞运营效果、业务安全运营效果以及供应链攻击防护实践等方面介绍了当前众邦银行的网络安全实践，并提出了互联网银行网络安全创新性的建设思路。

武汉大学信息管理学院教授洪亮发表了以《基于知识大图的金融风控关键技术与应用》为主题的演讲，演讲围绕着知识大图构建与管理、知识大图分析与表示以及金融风险防控应用等方面深入浅出的介绍了知识大图作为一种新生的技术形态，在金融风控领域的应用发展。他提出，当前知识大图在金融风控应用方面包括面向系统性金融风险监管的股权穿透、深交所发债企业风险预警以及交通银行商业票据融资欺诈识别等。

天融信科技集团解决方案中心总监于国强发表以《新形式下金融机构网络安全运营能力建设思路》为主题的演讲，演讲从新形式下金融机构网络安全特点、安全现状及面临的挑战、安全运营的设计思路、网络安全运营体系建设、网络安全运营制度建设、安全运营平台建设、网络安全运营评价体系建设、安全运营服务实施过程、安全运营实现效果以及天融信安全运营服务能力等方面进行全面的介绍。他表示，天融信安全运营中心是以技术、流程和人员有机结合，运用人

工智能、大数据、SOAR、UEBA 等先进技术，通过安全运营平台实现海量数据分析研判，持续性对安全风险及安全事件进行监测预警，解决各类安全风险，保障系统和业务安全稳定运行。

北京信利恒丰科技发展有限公司行业事业部副总经理朱悦坤发表以《网络安全合作经验分享》为主题的演讲，演讲围绕着金融行业需求特点、信利恒丰科技发展有限公司与天融信科技集团的合作经验分享、合作历程回顾以及未来合作方向等方面展开。她指出，在金融行业除了满足基础合规之外，未来在数据安全、XC 方向以及安全咨询规划等方面具有更大的项目需求。她提出，在合作过程中应利用天融信与信利恒丰双方优势，提高在项目中的竞争力，实现合作共赢！

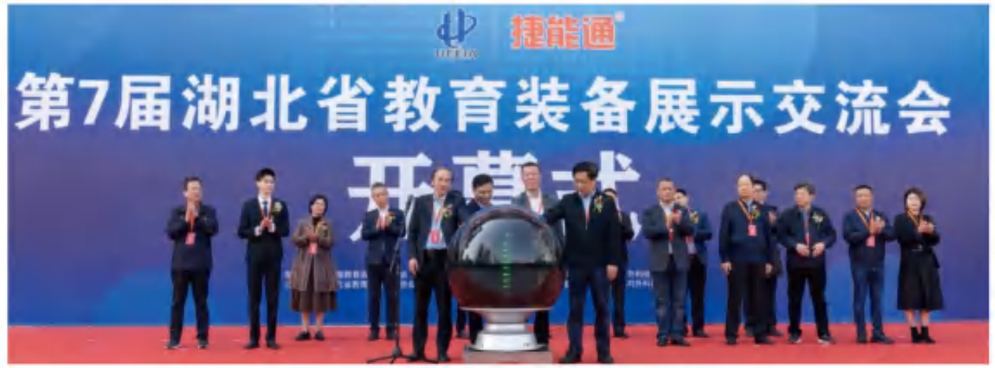
国任财产保险股份有限公司科技创新事业部总经理李斌发表以“网络安全保险为数字化转型保驾护航”为主题的演讲，李斌指出随着政策、监管的不断推进，国内网络安全保险市场发展越来越成熟。未来，要建立健全网络安全保险政策标准体系，加强网络安全保险产品服务创新，强化网络安全技术赋能保险发展，促进网络安全产业需求释放，培育网络安全保险发展生态。

为更好的推动网络安全与金融保险业快速发展，推动网络安全与金融保险业融合创新与示范，武汉市网络安全协会与东湖科技保险发展促进中心签订战略合作协议。武汉两大行业机构签订协议，是武汉网络安全与保险金融服务融合发展的标志性事件，是落实武汉作为国家网络安全人才与创新基地承载地和国家级科技保险创新示范区双重国家使命的创新举措。期待双方共同深入合作，制定系列规范标准，推出更多服务和产品，为省市数字经济发展保驾护航，为全国网络安全和科技保险工作融合发展探索出“武汉模式”。

随着我国发展环境的持续优化，网络安全保险步入快速发展新阶段，去年底，工信部会同银保监会起草的《关于促进网络安全保险规范健康发展的意见（征求意见稿）》。网络安全保险产品形态和服务模式日益多元，“保险服务 + 安全风控”模式日趋成熟，“安全防护 + 保险保障”模式加快探索落地。为了加快网络安全保险工作落地，落实双方行业组织达成的战略意向，由北京天融信科技集团、国任财产保险股份有限公司、亚泰保险经纪有限责任公司签订三方战略合作协议。未来，三方将在网络安全技术支撑、保险专业技术开发、保险经纪推广等方面开展深入务实合作。

金融业安全与否直接影响国家安全和社会稳定，而金融网络安全防护则是重中之重，随着金融行业信息化进程不断推进，势必会激发更多新的需求、面临更多新的挑战。作为本次大会承办单位的天融信科技集团表示，未来天融信将持续助力金融行业数字化转型，为金融客户构建高水平的安全防御体系，为金融行业安全稳定发展保驾护航。

我会团体标准在第 7 届湖北省教育装备展示交流会上正式发布



开幕式

江城三月春始足，梅花谢后樱花开。

四月，是武汉最美的时节，“樱”雄武汉重焕生机，在这春光明媚的日子里，第 7 届湖北省教育装备展示交流会于 4 月 1 日在武汉国际会展中心盛大开幕。

本届展会由中国教育装备行业协会指导，湖北省教育技术装备处、湖北省对外科技交流中心支持，湖北省教育装备行业协会、湖北省中小学校长协会主办，武汉市教育发展保障中心、湖北省学前教育研究会、武汉智能教育产业技术研究院、武汉市网络安全协会协办，湖北中科对外科技合作有限公司承办，本届展会由厦门捷能通光电科技有限公司总冠名。

活动中，我会专家委员会专家、本标准牵头起草人、湖北经济学院二级教授孙宝林，对我会团体标准《中小学信息化设备教学应用净化管理规范》进行了详细解读。

协会秘书长刘悦恒代表本标准发布机构宣读了关于发布《中小学信息化设备教学应用净化管理规范》团体标准的公告。

该团体标准从中小学信息化设备教学应用过程中发现的各种违法违规、网络谣言、诱惑性文字、弹窗信息、刷屏霸屏、网课爆破、捆绑软件、捆绑组件、广告信息以及收集个人信息等各种信息流进行监测与管理，建立一套适用中小学信息化设备教学应用净化管理的规范。为教育管理部门了解、掌握、分析和改进中小学信息化设备教学应用过程中的教学软件准入、管理、使用等环节提供参考依据，还为教学硬件、软件开发企业参与中小学信息化设备教学应用的开发，提升硬件制造、教学软件开发、应用软件开发水平等工作提

供指引。指导并规范中小学教育信息化设备教学应用净化管理工作，推动教育事业和教育信息化的教学应用安全、健康、协调发展。

标准起草单位：

武汉同德兴信息技术有限公司、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、湖北省教育信息发展中心、湖北省公安厅科技信息处、武汉市教育条件建设管理处、武汉市教育科学研究院、武汉市东湖新技术开发区教育发展研究院、武汉市标准化研究院、华中科技大学、武汉商贸职业学院、长江网、松滋市电教装备中心、洪湖市装备站、武汉市东西湖区教育局电化教育馆、新洲区教育局教育技术装备站、武汉宏焱高新科技有限公司、郑州新思齐科技有限公司、武汉弘博软件教育股份有限公司、广州视睿电子科技有限公司、奇安信科技集团股份有限公司、武汉安域信息安全技术有限公司、北京赛昇科技有限公司湖北分公司、武汉科云信息技术有限公司、河南职业技术学院、湖北省水果湖高级中学、湖北省水果湖第一中学、武汉市光谷实验小学、武汉东湖新技术开发区流芳幼儿园。

标准主要起草人：

孙宝林、夏群林、刘媛、刘悦恒、熊北平、雷春、何砚洲、胡露、马涛、艾威、陈克斌、曹毅、骆泓玮、宋莺、倪燕翎、罗欣、黄勇、李勇、崔文广、孙冉、丰婉伊、乔奇、王浩、庞博、李媛、文泽新、李纪云、邓太勇、方自安、胡磊、熊俊杰、宋小军、罗新豫、刘天梅、孔德勇、任道明、尹江发、张宇、周佑源、丁志鹏、何苗苗、李静、朱云云。

本届展会是湖北省教育行业的盛会，是教育管理者、教师与教育装备厂家、经销商、服务商面对面交流的平台，本次展会为期三天，全省教育行政、教育装备、电化教育、后勤管理、政府采购等部门负责人，以及各级各类学校负责人、一线教师等前来参观交流，预计参展及观展人数达万人次。

本次发布会后，我会秘书长刘悦恒接受了湖北经视采访。我会发布的本项团体标准得到了媒体的广泛持续关注，在起草至发布过程中湖北电视台综合频道、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。

2023 年武汉东湖网络安全保险专项工作培训会顺利召开

为深入学习贯彻习近平总书记关于网络强国的重要思想，积极迎接第八个全民国家安全教育日，增强全民国家安全意识和素养，夯实以新安全格局保障新发展格局的社会基础，进一步学习工信部会同银保监会起草的《关于促进网络安全保险规范健康发展的意见（征求意见稿）》，更好地开展数字资产保险网络安全工作。4 月 13 日，“2023 年武汉东湖网络安全保险专项工作培训会”在东湖科技保险发展促进中心顺利召开。8 家保险公司、13 家网安企业共同参与本次培训。

本次培训工作以“网络安全 + 保险”进行专题分享。武汉东湖科技保险发展促进中心主任孙智讲授了保险的基本原理，他结合三十多年的行业经验进行讲解，给大家带来新的启发和收获。武汉市网络安全协会数字资产保险网络安全工作部主任周韬讲解了网络安全基本概念和数字经济风险管理的探索和思考，使大家对数字经济中的网络安全风险有了更深层次的认识。

参会人员在培训后，针对网络安全与保险业融合工作展开了讨论。武汉市网络安全协会秘书长刘悦恒、东湖科技保险发展促进中心主任孙智就如何开展网络安全保险工作发言，就建立网络安全保险服务标准、网络安全保险产品创新、网络安全保险宣传和调研推广进行了交流。通过本次培训工作，加深了网络安全和金融保险领域专业知识的了解，激发了共同探索协同创新的动力，工作思路更为清晰，加快了我市网络安全与保险融合发展工作的步伐。

本次培训工作是进一步落实武汉市网络安全协会与武汉东湖科技保险发展促进中心双方战略合作协议的具体工作。今年 3 月 30 日，武汉市网络安全协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，共建东湖网络安全保险服务中心，共同开展网络风险管理研究和网络安全保险服务，为东湖和全市各类型单位提供网络安全保障。

本次工作培训会由东湖网络安全保险服务中心主办、武汉市网络安全协会和东湖科技保险发展促进中心承办。

2023 年武汉市智能汽车网络安全专项工作研讨会顺利召开

为积极贯彻《网络安全法》、《数据安全法》、《个人信息保护法》等法律规定，落实市委市政府重要战略部署，勇担科技自立自强使命，加强关键核心技术攻关，推动我市产业链创新链深度融合，规范汽车行业数据处理活动，保护个人、组织的合法权益，维护国家安全和社会公共利益，4 月 13 日，由武汉市网络安全协会主办的“2023 年武汉市智能汽车网络安全专项工作研讨会”顺利召开。

国家计算机网络应急技术处理协调中心湖北分中心、武汉市委网信办相关业务处室负责人，以及在汉整车厂商、检验检测机构、科研院所、高校、网络安全企业、通信运营商等近 30 家企事业单位代表莅临会议现场。

本次会议由武汉市网络安全协会秘书长刘悦恒主持，他向大家介绍了协会在智能汽车网络安全方面近期工作情况。

会议特邀了全国汽车行业知名专家与各位代表分享。原一汽、华晨、北汽高管，浙江远算科技有限公司首席专家何华潮老师向与会代表介绍了全国智能汽车行业发展情况。

作为总部设立在武汉的中央直管的特大型汽车企业东风汽车集团，近年来也持续发力智能网联车市场，本次会议特邀了集团技术中心副总工程师兼车联网信息安全 PTO 孙伟先生，他向参会嘉宾详细介绍了东风汽车集团智能汽车网络安全方面工作和发展情况。

中汽研汽车检验中心（武汉）有限公司副总经理姜春生介绍该公司智能汽车检验检测工作基本情况。 中汽研成立于 1985 年，是国务院国资委管理的央企，是具有行业影响力的汽车产业综合性服务机构，在智能网联车网络信息安全领域开展了大量基础性工作。

在汉智能网联车企代表之一，路特斯汽车信息安全总监熊吉，也向会议分享了路特斯在网络信息安全方面的经验和建议。

与会代表围绕我市智能汽车网络安全工作展开了深入讨论，国家工业信息安全发展研究中心，工信部赛宝华中实验室、武汉大学、华中科技大学、武汉理工大学、天融信等单位专家教授，纷纷谏言献策，在标准制定、人才培养、产教融合、专业实验室建设、平台搭建等话题提出了各自专业建议，会议还针对协会智能汽车网络安全专业委员会筹备工作展开了专题讨论，与会专家均表示愿意积极参与我市智能汽车网络安全相关工作。

凝心聚力、和志共识，本次会议旨在共同推进智能汽车与网络安全融合发展，努力形成我市智能汽车网络安全创新发展新模式，为我市智能汽车网络安全与数据安全发展提供智库支撑。

下一步，武汉市网络安全协会将继续把握行业发展动向，充分发挥专业性社团职能，带动网安产业，赋能智能汽车网络安全保障能力建设，为我市加固智能汽车网络安全防线贡献力量。

2023 年第一次会长轮值交接活动暨团体标准编制宣贯培训会顺利召开

4 月 27 日，武汉市网络安全协会 2023 年第一次会长轮值交接活动暨团体标准编制宣贯培训会在武汉安域信息安全技术有限公司会议室顺利召开。协会理事会成员、部分会员单位代表、以及申报了我会 2023 年团体标准立项申请的有关单位近四十人应邀参加了本次活动，活动还特别邀请了武汉市标准化研究院专家为与会来宾带来了关于团体标准编制的专题培训。

本次会议由武汉市网络安全协会秘书长刘悦恒主持。根据协会《章程》、《武汉市网络安全协会轮值会长工作制度》规定和协会第二届理事会第二次会议有关决议，协会副会长单位武汉安域信息安全技术有限公司为本季度轮值会长单位。活动中，秘书长代表协会向安域公司总经理周佑源授轮值会长牌。

周佑源会长向协会会员代表介绍了轮值工作安排。他从标准化体系建设、网络安全大讲堂、会员互动企业行、党建活动四个方面对轮值期间协会工作进行了规划，得到了与会代表的一致支持。

本次会议，还特别邀请了本年度新入会的各会员单位代表，举行了迎新仪式。周会长代表协会对 2023 年协会第一批新会员表示热烈欢迎，希望各单位以协会为家，群策群力，共同为武汉网络安全事业贡献力量。

针对团体标准编制工作，我会特别邀请了武汉市标准化研究院团体标准发展促进中心主任、正高级工程师黄勇老师，为大家分享了《团体标准编制工作解读》的专题培训。黄老师详细讲解了《标准化法》等国家法规，并介绍了团体标准的法律地位和适用范围，对大家编制过程中出现的疑问，通过真实案例一一解答。通过本次专题培训，进一步增强了协会成员单位参与标准化工作的信心和动力，提升了标准编制能力，申报单位纷纷发言，愿在协会的统一组织下，努力为我市网络安全标准化工作开辟新的局面。

武汉市网络安全协会作为全市网络安全产业的代表，具备全国团体标准信息平台团体标准发布资格，今年在全省教育装备展上顺利发布了《中小学信息化设备教学应用净化管理规范》（T/WHCSA 001—2023）团体标准，并于 3 月 17 日发布了《关于开展 2023 年武汉市网络安全协会团体标准立项征集的通知》，目前各会员单位正积极参与申报。

本次活动的成功举办，进一步调动了广大会员参与协会各项工作的积极性，加深彼此了解和协作，提升了协会服务会员的能力。期待后续在新任轮值会长的带领下，协会不断拓展生态圈朋友圈，各项工作不断规范化标准化，切实为主管部门和各会员单位发展做好桥梁纽带做好支撑服务。

武汉市网络安全应急技术支撑单位自律公约

第一条 为贯彻落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《国家网络安全事件应急预案》等国家网络安全相关法规，加快构建超大城市网络安全应急指挥管理体系，强化武汉市网络安全应急技术支撑队伍建设，特制定本公约。

第二条 武汉市网络安全应急技术支撑队伍（以下简称：支撑队伍）是由市委网信办和市公安局共同遴选出的外协队伍，是我市构建超大城市网络安全应急指挥管理体系的重要组成部分。

第三条 各支撑队伍应坚持中国共产党的全面领导，自觉遵守国家有关的法律、法规和政策，做到政治过硬、专业精干、纪律严明，在筑牢我市网络安全防线中持续发挥“招之即来、来之能战、战之必胜”的工作作风。

第四条 倡议各支撑队伍从促进我市网络安全事业发展的高度出发，自觉加入本公约，履行自律义务，创造良好的队伍发展环境。

第五条 各支撑队伍应具有完备的人员管理、设备管理、保密管理等内部管理制度，常态化开展人员培训教育和实战化演练，不断增强专业能力和职业素养。

第六条 各支撑队伍应建立数据集中、情报共享、支撑联动、共保平安的协作机制，实现网络安全保障工作互补互进、增质增效。

第七条 各支撑单位应加强网络安全监测预警、防控等技术研究，不断升级技术装备，为网络安全应急响应工作提供强有力的技术支撑。

第八条 本公约由武汉市网络安全协会制定，并负责解释、组织和实施。

第九条 本公约于 2023 年 3 月 3 日第二届理事会第二次会议全票通过，自 2023 年 3 月 6 日起试行。

已签订自律公约单位：

北京天融信网络安全技术有限公司	北京长亭科技有限公司
杭州安恒信息技术股份有限公司	曙光网络科技有限公司
武汉安域信息安全技术有限公司	北京山石网科信息技术有限公司
北京神州绿盟科技有限公司	武汉安经纬业信息安全技术有限公司
亚信科技（成都）有限公司	光谷技术有限公司
三六零数字安全科技集团有限公司	恒安嘉新（北京）科技股份公司
武汉华康科技有限公司	湖北省网络信息安全技术管控中心
湖北东方网盾信息安全技术有限公司	湖北省电子信息产品质量监督检验院
武汉安天信息技术有限责任公司	武汉网信联盾网络安全技术中心（有限合伙）
武汉市德发电子信息有限责任公司	武汉明嘉信技术有限公司
奇安信网神信息技术（北京）股份有限公司	武汉联钢科技有限公司
武汉烽火信息集成技术有限公司	湖北星野科技发展有限公司
武汉云视科技技术有限公司	武汉光谷信息技术股份有限公司
深圳海云安网络安全技术有限公司	北京安博通科技股份有限公司
武汉吧哒科技股份有限公司（原四通）	蓝芽网络技术（湖北）有限公司
武汉易通科技有限公司	上海观安信息技术股份有限公司
湖北中网科技有限公司	上海文鳐信息科技有限公司
湖北珞格科技发展有限公司	武汉京伦科技开发有限公司
智网安云（武汉）信息技术有限公司	北京启明星辰信息安全技术有限公司
鸣飞伟业技术有限公司	湖北梆梆安全科技有限公司

武汉市网络安全协会轮值会长工作制度

为进一步促进协会日常工作的开展，充分发挥协会会长、副会长、理事的职务作用，调动广大会员的积极性和团队协作精神，推动协会的制度化建设，特制定本制度。

一、会长轮值安排

1、副会长单位按理事会决议固定轮值，理事单位按自身意愿申请轮值，轮值安排由理事会决定。实行轮值会长制度后，协会会长单位、会长、法人代表等相关备案信息不做变更；协会秘书处的办公地点、财务制度保持不变。

2、每季度为一个轮值时间单位。

3、轮值单位需派驻专员借调协会参与工作。派驻期间，派驻人员全职在协会上班，作为协会工作人员接受协会管理，可以代表协会轮值会长开展工作，根据协会《章程》第四十六条规定，协会工作期间薪酬待遇由原单位解决，原则上不低于借调前待遇，协会每月给予工作津贴。

二、轮值会长工作职责

1、轮值期间牵头组织策划一项大型活动，牵头组织 1-2 次会员单位互访交流活动等。

2、处理协会的重大事件和应急突发事件。参与协会日常管理工作。

3、轮值前提交工作计划，轮值结束时向理事会提交工作报告。

三、轮值工作考核、评比、交流

1、在轮值结束后，由理事会及秘书处成员，根据当期轮值会长日志记录考核各轮值会长在任职期间的工作情况，并予以考核评分。

2、根据各轮值会长及派驻专员在任期间的考核成绩进行评比，选出本年度优秀轮值会长及派驻专员，协会在年终予以嘉奖。

3、协会定期安排优秀轮值会长单位进行经验总结与交流，相关成果结集成册向主管部门和会员单位报送。

本制度于 2023 年 3 月 3 日第二届理事会第二次会议全票通过试行。

安天移动安全成为八家通过中国信通院“能力验证计划”的企业之一

近日，中国信息通信研究院（以下简称“中国信通院”）泰尔终端实验室，依据 ISO/IEC 17043：2010《能力验证提供者能力的要求》（CNAS-CL03《能力验证提供者认可准则》）对全国主要 APP 个人信息保护检测机构的检测能力进行了考核评估，安天移动安全成为八家通过中国信通院评测的企业之一

序号	测试结果名单
1	北京百度网讯科技有限公司
2	北京卓易讯畅科技有限公司
3	北京翔辉安全科技有限公司
4	北京捷兴信源信息技术有限公司
5	北京智游网安科技有限公司
6	北京数智鑫源科技有限公司
7	北京速云科技有限公司
8	**武汉安天信息技术有限责任公司**

（排名不分先后，按照笔划排序）

为切实提升机构检测技术和服务水平，提高行业个人信息保护水平，2022 年 11 月，中国信通院泰尔终端实验室开展了“移动互联网应用程序（APP）用户权益保护测试能力验证计划”。参加本次能力验证计划检测机构以《移动互联网应用程序（APP）用户权益保护测评规范》《信息安全技术移动互联网应用程序（APP）收集个人信息基本要求》等标准为依据对样品 APP 进行测试。

基于十余年的技术积累和实战经验，目前，安天移动安全针对当前移动应用风险问题已初步形成系统性发现能力，建立了细粒度的移动互联网应用问题取证标准，采用终端侧本地规则引擎和云端检测引擎的双引擎战略，实现终端用户侧真实威胁态势的感知能力和实时的威胁处置能力，能够精准定位恶意代码、模块、SDK 及各类小程序、快应用等侵害用户权益问题，并最终通过中国信通院本次测试评估。

在此次能力验证测试中，安天移动安全仅展示了部分检测技术和能力，本次获得中国信通院的认可，既是安天移动安全在移动应用风险检测技术方面综合能力的体现，也是对安天移动安全在移动生态个人信息保护领域核心技术优势的肯定。

作为网络安全的助推者，为保障广大用户合法权益，一方面，安天移动安全“安鉴”风险检测预警平台将及时跟进政策法规和检测细则的更新并进行专业解读，帮助开发者了解监管及合规政策，并提供整改申诉、复测入口，实现检出规则和政策同步迭代。

另一方面，安天移动安全将持续加大研发投入和技术人员能力提升，精准定位恶意代码、模块、SDK 及各类小程序、快应用等侵害用户权益问题，提前布局技术趋势的前沿领域安全。并积极配合工信部、中国信通院、泰尔终端实验室等监管部门开展 APP 用户权益保护检测技术支持和相关保障工作，与移动产业链各方一同保障用户权益，共建纯净健康的移动互联网生态。

洪山区副区长袁永康率队走进吧哒科技

为进一步提升企业服务精准度，2023 年 1 月 30 日，武汉市洪山区副区长袁永康、武汉洪山城市建设投资有限公司董事长彭学斌、武汉市洪山科技投资有限公司党支部书记、董事长喻峰、区政府办、区科经局、区商务局、街道负责人赴吧哒科技走访调研。

调研期间，吧哒科技总经理陈立军向莅临领导汇报了公司成立 24 年间各阶段发展历程，分享了“大信创”时代将至的背景下，智能化和信息化集成相结合的公司优势，以及信服易备产品实力和公司生产运营情况。

洪山区政府相关负责人及与会领导纷纷表示，针对吧哒科技提出的产业合作等需求，将积极沟通协调，在稳健的政策支持下，为企业做好服务工作，推出更多精准推介和人才交流活动，在合理合规的基础上促成更多合作。

洪山区副区长袁永康对吧哒科技工作成果和运营形势表示肯定。他指出，信创产业是国家战略，也是新基建的重要组成部分，吧哒科技从最初做系统集成转型做运维，再到研制生产自己的产品，从做服务到信服易备应用到众多领域，现已扎根市场，成为洪山区重要科创力量。新的一年，望吧哒科技坚定信心，相关部门将一如既往提供优质高效服务，协调解决实际问题，创造产业技术、科技创新、人才培养的有机融合，共同加快推进企业实现更好发展。

烽火入选“数字政府建设赋能计划—智慧应急推进组”首批成员单位

近日，为推动我国智慧应急深度发展，中国应急管理学会信息化工作委员会、中国信息通信研究院、中国通信标准化协会联合主办的“数字化赋能应急管理创新实践论坛”成功召开，本次活动汇聚了行业权威机构、专家学者、厂商代表等，共同探讨智慧应急领域的技术创新、案例实践及发展机遇。

会上，中国应急管理学会项目部主任高崇峰、中国信通院云大所副所长栗蔚分别致辞，提出要大力促进数字技术与应急管理业务的深度融合，推动应急管理信息化建设高质量、高水平发展。此外，会议宣布“数字政府建设赋能计划—智慧应急推进组”正式成立，烽火凭借在智慧应急领域的综合实力成功入选首批成员单位，烽火应急专家徐凤祥入选首批技术专家名单。

烽火是中国应急管理学会信息化工作委员会的牵头单位。自信工委成立以来，烽火一直致力于运用云计算、大数据、互联网、人工智能等数字技术推动“智慧应急”的建设，助力政府部门提升公共安全管理能力及应急管理能力，为产学研用的多方合作提供了有力支撑。近年来，烽火凭借在智慧应急、大应急数据治理、应急通信等方面的深厚积淀，紧跟应急业务需求变化，落地了一系列应急信息化建设项目，积累了丰富的经验。

江岸区人民政府与武汉联通携手发力数智化转型

3 月 24 日，武汉市江岸区人民政府区长余志成率队到武汉联通开展调研交流。江岸区人民政府副区长李绪杰、湖北联通党委委员、副总经理、武汉联通党委书记、总经理刘伟锋等出席相关活动。

活动中，双方代表参观了湖北联通 5G^n 数字化创新体验中心，通过丰富生动的 5G 应用场景体验，全面分享了武汉联通在发展 5G 新基建方面的基本情况、场景应用、技术攻关、创新生态等情况。通过集中展示，让大家充分了解了 5G 通信技术服务的新理念、新成果。

参观后，双方代表开展了深入交流。武汉联通产

业互联网运营中心总经理王晓燕作了题为《武汉联通助力"数智江岸"建设》专题汇报。从中国联通能力体系、聚焦武汉深耕江岸以及数智江岸建设蓝图三个部分深入阐述了新时代数字央企优质的服务能力和创新动能。

随后，江岸区人民政府副区长李绪杰与武汉联通党委委员、副总经理李拥斌代表双方签署《江岸区人民政府与中国联合网络通信有限公司武汉市分公司加快"十四五"期间数智江岸建设战略合作框架协议》。

根据协议，双方将携手发挥各自优势，深化务实合作，加强在数字信息基础设施、数字政府、智慧城市、工业互联网、数据安全等重点领域的深度合作，共同推进实现"汉口之心、美好江岸"的总体目标。

余志成首先肯定了武汉联通长期以来在推进江岸基础设施建设、做优城区网络运营服务、赋能数字经济产业等多方面取得的成效。他表示，江岸作为首善之区，肩负着市委市政府赋予的"主城做优"，助力打造数字经济一线城市的重要使命。江岸作为枢纽要地、产业重地、创新高地，"十四五"期间正迎来前所未有的战略机遇，区政府将用心用情提供最优政策、最佳环境、最好服务、最强保障，大力支持武汉联通深耕江岸、蓬勃发展，武汉联通以"数智活水"持续浇灌"发展之树"，必会在江岸收获丰硕的果实。

刘伟锋表示，近年来，武汉联通以新战略为指引，乘新一代信息技术发展之东风，始终牢记"数字信息基础设施运营服务国家队、网络强国数字中国智慧社会建设主力军、数字技术融合创新排头兵"之定位，积极拥抱数字经济，将"大联接、大计算、大数据、大应用、大安全"作为五大主责主业，在主动融入武汉市，特别是江岸区数字经济建设主战场中提出联通方案，在积极服务"六稳""六保"工作任务中努力展现联通担当。武汉联通将以此次战略协议签约为契机，在区委、区政府的正确领导下，加快"数智江岸"工作推进，力争尽早形成一批标志性成果，为加快建设"汉口之心、美好江岸"，助力打造新时代英雄城市贡献武汉联通更大力量。

海云安在中国金融业开源技术应用与发展论坛上荣获"金融开源践行者"表彰

3月28日，全球金融科技大会——中国金融业开源技术应用与发展论坛在新动力金融科技中心举办，本次会议旨在进一步贯彻落实人民银行等五部委联合发布的《关于规范金融业开源技术应用与发展的意见》，搭建高层次、高质量开源领域产学研用交流对接平台，挖掘金融领域开源应用深度痛点需求，分享金融领域开源治理最佳应用实践。会议由北京国家金融科技认证中心、北京金融科技产业联盟开放原子开源基金会、国家工业信息安全发展研究中心联合主办。

本次大会由北京国家金融科技认证中心实验中心负责人李博文主持，大会邀请了知名的金融机构、科技公司、开源社区和专家学者分享他们在开源技术方面的最新进展、经验和挑战，并探讨中国金融业在开源技术应用与发展方面的机遇与前景。会上同时邀请了开源安全厂商，分享他们在金融业务中使用开源技术的经验和成果，展示了开源技术在金融创新、风险管理、数据分析等方面的价值和潜力。海云安作为开源安全厂商代表受邀参加此次盛会，并获得"金融开源践行者"表彰。

开源是指软件或硬件的源代码可以被公开访问、修改和共享的一种模式，开源可以提高金融业的创新能力和效率。通过使用开源的技术和平台，金融机构可以快速开发和部署新的产品和服务，满足客户的需求和期望。与此同时，开源也存在一定的安全风险。由于开源软件的源代码是公开的，黑客可以利用其中的漏洞进行攻击。使用者需要及时更新开源软件，或者使用安全审计工具检测潜在的风险。

势在·人为
融信天下合作伙伴大会 2023 盛大召开

3 月 30 日，融信天下合作伙伴大会 2023 在武汉盛大召开。大会以“势在·人为”为主题，邀请省市有关领导、专家学者、合作伙伴齐聚一堂，多维度共话网安产业趋势，分享最新前沿技术，展望网安未来、共话产业趋势。

中共中央、国务院近期印发的《数字中国建设整体布局规划》明确指出，发展数字中国，推动数字经济，须以数字化驱动安全治理变革，加快构筑自立自强的数字技术创新体系，构建可信可控的数字安全产业生态，以数字化安全的体系、技术、能力、产品，筑牢数字化安全防线。如今，网络空间安全已成为国家安全体系中的重要组成部分，也是加快建设数字中国、推动数字经济发展的重要保障。

武汉市东西湖区区长周明在致辞中表示，党的二十大报告对加快建设制造强国、网络强国、数字中国，促进数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群做出了重大战略部署。我国数字经济正在迈向深度应用、合规发展和普惠共享的新阶段，在数字赋能引领高质量发展的同时，网络安全治理与建设作为网络强国、素质中国的底座，将在未来的发展中承担着托底的重担。

2016 年，全国唯一的国家网络安全人才与创新基地落户在东西湖区，去年，网安基地成功入选工信部网络安全技术应用试点示范项目。天融信科技集团作为国内网络安全行业领导企业，也是首批入驻网安基地的企业，为基地产业发展注入了强大动能和活力。

天融信科技集团董事长兼 CEO 李雪莹博士在《相融共创 赋能未来》主题演讲中表示，当前，我们处于一个数字化快速发展的时代，网络安全对整个数字经济和数字建设至关重要。她指出信息化技术应用、安全威胁变化、国家政策法规要求是驱动网络安全产业发展的三大动力。天融信 27 年来与网络安全产业同发展共成长，致力于成为中国领先的网络安全、大数据与云服务提供商。

天融信面向新技术、新场景，运用新技术、新应用，一路创新。同时，天融信与时俱进，不断超越自己。从专注网络安全，发展到提供云计算基础设施；从提供产品和方案，发展到安全能力交付；从面向基础网络场景，扩展到覆盖车联网、物联网、工业互联网（包括工业控制系统）等新场景。打造全产品系列，面向全业务方向，天融信产品技术的创新超越充分体现了网络安全产业国产化、行业化、服务化、智能化的发展趋势。

天融信顺应数字化发展趋势，在营销领域积极超越创新。公司持续推进全行业营销，开展全区域覆盖。通过行业的横向拓展、纵向深耕，区域的地市下沉，不断突破。面对新发展，运用新机制，形成亚直销加合作伙伴营销，原厂服务加授权合作伙伴服务的新格局。

最后，李雪莹博士希望通过天融信 27 年的积累赋能合作伙伴成长发展，进而为更多客户数字化发展进行安全赋能，共同助力数字中国建设。

公安部第一、第三研究所原所长、中国计算机学会计算机安全专业委员会荣誉主任严明发表《紧握“十大要点”推进关基保障》主题演讲。他表示，《关键信息基础设施安全保护条例》（以下简称“条例”）是贯彻落实习近平总书记关于网络强国重要思想的具体措施，也是近年来国家网络安全和信息化工作成功经验的制度化提升。他提出要紧握条例“十大要点”，为我国深入开展关键信息基础设施安全保护工作提供有力法治保障。

北京师范大学法学院博士生导师、中国互联网协会研究中心副主任吴沈括带来了《数据跨境安全治理与合规风控》主题分享。他表示，由于企业全球化运营、国家数字主权以及国家安全等原因，数据跨境安全治理和合规风控日益重要。目前企业数据合规仍存在数据资产不明、生态场景不清、部门沟通不足、业务协同不高等痛点，需要从评估、认证，到标准合同等方面入手解决。自 2015 年起至今，中国颁布了多项有关数据安全和数据保护的政策战略和法律法规，为解决企业跨境数据合规的常规痛点提供了指导方针。从国际上来看，各个国家都开展了相关的数据跨境国别研究，为中国法下的数据出境安全合规提供了借鉴意义，同时中国也颁布了有关中国数据出境规则的法律、行政法规以及其他规范。这也说明，目前的合规风控体系不仅需要更新理念，更需要有配套机制和全球格局。

IDC 中国研究总监王军民作《中国网络安全市场发展趋势》主题演讲，他指出，数字化转型已经成为全球发展的趋势，从当前全球网络安全形势来看，数字世界中安全问题凸显，已经成为全球各国数字化建设的“绊脚石”。当前，我国已经进入数字中国快速建设的进程中，《数字中国建设整体布局规划》中强调，到 2025 年，数字安全保障能力全面提升，同时，强化数字技术创新体系和数字安全屏障“两大能力”。由此可以预期，未来几年，中国企业级客户的数字安全建设将迎来新一轮发展高峰。数字安全建设刻不容缓，也必将成为我国各行各业在数字化发展过程中必须关注的热点。

天融信科技集团副总裁耿硕在《聚势汇力 事在人为》主题演讲中表示，近年来，数字经济发展规模之大、速度之快、涉及面之广、影响程度之深有目共睹。网络安全产业发展全面提速，加快迈进高质量发展阶段，乘借着此东风之大势，天融信自渠道业务开展五年来，在合作伙伴侧对于拓展、人才、品牌、产品及解决方案的积累，赋能合作伙伴共成长，助力客户数字化转型发展，全面推进数字中国建设。在对 2023 年展望时，他阐述了人为的含义，知势以悟道，谋事以做局，天融信会通过对渠道政策、业务流程、人才培养、市场资源等一系列方面进行优化和投入，保障全国的合作伙伴能够享受到更高效、更有力度的支持。2023 年，天融信将会维护公正公平的渠道秩序，保障合作伙伴“有投入、有收获”，与合作伙伴一同，打造共创、共赢、共享的渠道业务新生态。

天融信科技集团副总裁吕延辉在分享《聚力赋能 携手共进》演讲中指出，天融信经历 27 年发展，不断拓展需求场景广度和客户覆盖深度，将产品和服务能

力充分与客户实际需求场景进行结合，形成了目前的红•黑矩阵。矩阵下方黑色部分代表我们的产品体系，分为网络安全、大数据和云服务三大业务板块，包含 100 多款产品、1000 多个型号；上方红色部分代表我们的解决方案，覆盖行业、合规、专项、新技术、新场景等五大类共三十小类。同时，针对国产化替代需求，我们也有适用于不同场景的信创解决方案和丰富的天融信昆仑系列信创产品体系。红•黑矩阵整体代表的是构成天融信“全产品系列、全业务方向、全行业营销、全区域覆盖”的“四全”体系的核心能力图谱，未来它还将不断进化。

天融信科技集团董事长兼 CEO 李雪莹、天融信科技集团副总裁耿硕，邀请 IDC 中国研究总监王军民一起，与合作伙伴代表北京汇志凌云数据技术有限责任公司、联强科技有限公司、伟仕佳杰（中国）、河北乐讯电子科技有限公司共同启动 2023 聚势•燎原启动仪式。

“聚势•燎原”活动，是天融信 2023 年为合作伙伴开展的系列活动。随着活动启动，天融信将在全国百余城市、地县进行渠道合作政策、产品及解决方案的宣讲，同时持续开展对合作伙伴赋能培训，为合作伙伴培养网络安全人才；与合作伙伴一同举办行业沙龙，共同面向细分行业市场拓展客户；布局授权服务中心，将更快速、更专业的服务下沉到地市区县，为合作伙伴打开服务市场之门，聚合作伙伴之势，燎网络安全之原。

传捷报！共奋进！ 珞格科技荣获 2022 年度测评机构 能力验证“优秀单位”

在 2 月 21 日召开的全国网络安全等级保护测评体系建设会议上，湖北珞格科技发展有限公司被评为“2022 年度测评机构能力验证优秀单位”之一！作为湖北省信息网络安全协会理事单位，珞格科技凭借过硬的综合实力以及雄厚的技术实力，在 2022 年也多次荣获，多省网络攻防实战演习“优秀单位”、及诸多奖项。

本次活动是目前全国规模最大的网络安全等级保护测评能力验证活动；珞格科技从 32 个省、自治区、直辖市的 226 家测评机构，共 1340 名网络安全等级保护测评人员与攻防人员中脱颖而出。

本次能力验证活动分为测评能力考核与 CTF 竞赛两部分，在当前“三法一条例”的实施背景下，特别增加数据安全的测评内容，对测评机构的数据安全测评能力进行普查摸底。

在能力验证活动中，不仅全面考察等级测评行业从业人员的理论水平，更考察实际业务能力，探索“以比促训、以赛促战”的模式，引导测评机构积极适应新政策、新技术、新形势，为进一步推进行业高质量发展、保障国家网络安全等级保护工作奠定扎实的基础。

党的二十大指出：应推进新型工业化，加快建设

制造强国、网络强国。在数字化转型关键期，中国网络安全产业发展呈现出国产化、行业化、服务化与智能化的“四化”趋势。

党的二十大以来，“国家安全”的地位在国家治理现代化中得到进一步彰显。在新机遇、新阶段和新要求下，我国国家安全亟须应对的风险和挑战也更加错综复杂。如今数字化转型正在加速推进，数据成为继土地、劳动力、资本与技术等之后的第五大生产要素，数据安全亦成为国家安全的重要组成部分。

在未来，珞格科技将会一直秉承“质量为先、信誉为重、管理为本、服务为诚”的价值理念，持续深入各行各业，为各行业客户提供针对性的数据安全运营解决方案，协助客户完善数据安全防御体系，保障客户复杂系统和复杂交易的可持续发展，提升数据管理能力，赋能数字化转型发展，推进网络强国建设！

武汉安域全员培训暨年度会议圆满举行

2023 年 3 月 5 日至 3 月 7 日，武汉安域开展为期三天的全员培训暨年度会议。

本次会议以“战略目标落地及组织能力提升”为主题，以“小组共创”为手段，通过桌面创意摆放、价值观故事分享、价值观情景剧表演等环节，创造集体沟通互动的机会，增强团队凝聚力，为推动企业健康持续发展奠定了坚实的基础。

3 月 6 日下午，董事长叶全军带领大家一同回顾安域十年发展历程，正式发布全新升级的使命、愿景与价值观，提出对文化践行的期望，并激励大家共同为安域更好的明天努力奋斗！

3月7日上午，总经理周佑源作2022 年度工作总结，全面回顾过去一年取得的成绩，向所有辛勤工作在各个岗位的员工表示衷心感谢。同时宣贯未来三年战略目标，希望大家继续保持工作热情，持续加强团队协作力，凝心聚力共赴新征程，成为湖北省安全服务领先企业。

会上，公司对团队优胜冠军小组奖项、2022 年度优秀员工奖项、提供商机特别奖项及网络与信息安全管理员分别进行表彰，并颁发荣誉证书等奖励。

绿盟科技与长江职业学院校企合作签约

为加强校企深度合作，探索协同育人机制，助力专业发展。5 月 24 日，北京神州绿盟科技有限公司与长江职业学院在武汉东湖网谷（绿盟科技武汉研发中心）举行校企合作签约暨校外实习基地授牌仪式。长江职业学院党委委员、副校长张俊，绿盟科技湖北代表处首席代表张敬民参加仪式。

张敬民对张俊一行表示热烈欢迎，介绍了绿盟科技的发展历程、现有员工规模、主营业务及未来发展规划，并表达了愿与长江职业学院数据信息学院真诚合作的愿望，希望借助企业在行业中的优势和丰富资源助力信息安全技术应用专业的发展，发挥校企协同育人机制的作用，合作培养更多满足企业需求的信息安全技术应用人才，以缓解当前我国信息安全人才严重不足带来的压力，共同维护健康安全的网络生态。

党委委员、副校长张俊代表校方致辞，介绍了学校的发展情况和办学成果。他表示，学校高度重视产教深度融合、校企合作，希望企业方能够利用行业优

势，与学校开展广泛的合作，共同参与人才培养全过程。他强调，签约仪式是一个好的开端，后续学校和企业应围绕人才培养、师资互聘、项目研发等开展全方位、深层次的合作。

未来，双方将充分发挥和整合优势资源，突出校企“双主体”育人特色，共同探索专业特色鲜明、集“产、学、研、训”为一体的人才培养模式，为形成人才培养、技术创新、产业发展的良性生态链而不断努力。

武汉市网络安全协会 2023 年第一批新增会员介绍

1. 武汉赛宝工业技术研究院有限公司

武汉赛宝工业技术研究院有限公司成立于 2016 年 5 月，注册资金 500 万元，总部位于广州，是工业和信息化部电子第五研究所设立在武汉市的分支机构。公司作为从事工业和信息化产品质量与可靠性研究和检测的专业的第三方检测机构，在计量校准、软件测试、可靠性检测、环境适应性检测、认证、分析评价等方面开展技术咨询、技术推广、技术服务。

2. 武汉明嘉信技术有限公司

武汉明嘉信技术有限公司（以下简称“武汉明嘉信”）于 2007 年成为省内首批网络安全等级保护测评专业机构之一。测评人员先后参加过公安部测评中心、省公安厅等单位组织的相关网络安全等级测评培训，掌握相关管理规范和技术标准，熟悉等级测评的方法、流程和工作规范等方面的知识，并具备依据测评结果做出专业判断及出具等级测评报告等文档的专业技能。

武汉明嘉信一直致力于客户服务水平及信息安全水平的持续提升，已取得 ISO9001 质量管理体系认证证书、ISO20000 信息技术服务管理体系认证证书、ISO27001 信息安全管理体系认证证书、CCRC 信息安全服务资质认证证书（安全运维）、CCRC 信息安全服务资质认证证书（风险评估）、CCRC 信息安全服务资质认证证书（应急处理）。

3. 北京启明星辰信息安全技术有限公司

北京启明星辰信息安全技术有限公司成立于 2000 年，总部位于北京，主要经营范围：网络、计算机软硬件的技术开发、服务、转让、咨询、培训；承办展览展示；承接计算机网络工程；销售开发后的产品、五金交电、电子元器件、计算机软硬件及外围设备；信息安全设备的设计开发、生产、服务和维修；货物进出口、代理进出口；机械设备租赁（不含汽车租赁）。（企业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；不得从事本市产业政策禁止和限制类项目的经营活动）

北京启明星辰信息安全技术有限公司员工超 3500 人，在全国各省份均设有分支机构，拥有覆盖全国的营销体系和技术支持中心。在武汉市设有独立法人：武汉启明星辰信息安全技术有限公司，办公场地面积 516 平方米，共 50 人，网络安全服务 35 人，下设技术部、销售部、商务行政等部门，与网络安全应急技术支撑相关的部门有技术、销售等部门，分别负责技术服务和业务对接工作。

4. 武汉联钢科技有限公司

武汉联钢科技有限公司是一家从事网络信息软件开发，互联网数据服务，电子产品销售等业务的公司，成立于 2006 年 02 月 14 日，公司坐落在湖北省，主要经营范围为：网络与信息安全软件开发；互联网数据服务；电子产品销售；计算机软硬件及辅助设备批发；安防设备销售；通讯设备销售；网络设备销售：消防器材销售：农副产品销售；工艺美术品及礼仪用品销售（象牙及其制品除外）；普通机械设备安装服务：技术服务、技术开发、技术咨询、技术交流、技术转让、技术推广：广告设计、代理；广告制作；广告发布；平面设计；专业设计服务；企业形象策划；市场营销策划；网络技术服务；信息系统运行维护服务；信息系统集成服务；人工智能双创服务平台：互联网安全服务；物联网应用服务：数字文化创意内容应用服务；区块链技术相关软件和服务；数据处理和存储支持服务；物联网技术服务；信息技术咨询服务；数字内容制作服务（不含出版发行）：计算机系统服务：消防技术服务；安全技术防范系统设计施工服务；动漫游戏开发；软件开发；计算机及通讯设备租赁；办公设备租赁服务。

5. 武汉市德发电子信息有限责任公司

武汉市德发电子信息有限责任公司（Wuhan Defa Electronics Information co. Ltd）成立于 1994 年，注册资金 3000 万。是一家提供信息系统解决方案、IT 应用软件研发与销售、IT 技术支持与维护解决方案，以及为各行业客户提供云上整体解决方案，云战略咨询、云架构规划与设计、业务上云迁移部署、云运维管理、云容灾备份等服务的高新技术企业。

作为华中地区系统集成与 IT 服务领域的领导企业，德发公司重点为国家政府部门、安全部门、教育行业、企业客户等提供大型信息化建设、网络建设及安全解决方案；为政府和企业客户提供客户管理、门户网站、信息资源平台建设和决策支持等方面定制应用软件开发及解决方案；为各行业客户提供信息化运营支撑系统、数据中心等 IT 运维服务。经过 20 余年稳定健康的发展，德发公司分别在湖北、湖南、江西、云南、贵州、四川、重庆等地建立服务站。汇集了一批具有丰富经验的企业管理、主机维护、网络设计、项目实施、软件开发等高级技术和管理人才，建立起一支对 IT 技术发展趋势、软件产业有深刻体验和认识，并拥有丰富

行业经验和技术知识的优秀人才团队，培养了一批高素质的业务专家和技术专家。目前员工队伍超过300人，其中十多位拥有高级项目经理职称与高级工程师职称，本科及本科以上学历人员占85%。

6. 湖北连邦云创科技有限公司

湖北连邦云创有限公司成立于2018年，总部位于武汉洪山区珞瑜东路特一号。湖北连邦云创作为一家专业的信息化技术服务公司，利用云计算、大数据、物联网等技术，帮助政府、企业等客户实现服务转型及数字化转型。公司拥有专业的技术团队和完善的服务网络，根据客户需求及市场调研，进行技术研发及服务输出。公司成功研发了多款行业软件，其中就包括维护农民工及低保居民等弱势群体利益的软件系统，通过信息技术助力相关政府部门做好民生保障工作，并受到用户和领导的一致好评。

7. 武汉同捷信息技术有限公司

武汉同捷信息技术有限公司位于长江经济带核心城市——江城武汉，公司秉承“持续为客户创造价值、打造一流的信息化服务能力”的企业精神，致力于成为华中地区领先的信息化综合服务商。

同捷公司自成立以来，始终坚持技术创新，自主研发了产品数据管理系统、工艺数据管理系统、生产工单管理系统等20余项软件著作产品，先后通过了国家双软企业认定、高新技术企业认定、科技型中小企业认定，并多次荣获武汉市“守合同重信用企业”荣誉。公司主要业务方向包括了智能制造、研发系统、政务服务及网络安全四个板块，产品及解决方案广泛应用于制造企业、国防军工、政府机关、医疗机构等领域。为用户提供CAD、PLM、CAPP、MES、DLP及身份认证、网络安全、数据库安全等专业信息化产品及个性化交付服务、系统运维保障服务等一站式信息化整体服务。

8. 湖北公众信息产业有限责任公司

湖北公众信息产业有限责任公司成立于2004年9月。公司同时挂牌“中电信数智科技有限公司湖北分公司”、“中国电信股份有限公司湖北产业数字化研发中心”，注册资本总计人民币5000万元，总部坐落在金银湖航天路9号。2015年底，公司被委托运营中国电信ICT区域服务交付（武汉）中心，“立足本省、辐射周边”，重点辐射华中和西南地区，助力提升全网业务交付及服务能力。

公司主要从事信息领域软件研发、系统集成和IT支撑服务，公司连续三年被评为武汉市软件百强企业，并致力于为政府、企业、金融、医卫等客户提供专业的信息化解决方案，提供覆盖网络集成、业务管理、信息管理、网络外包、安全管理、数据维护分析和增值应用服务等业界领先的产品与服务。

公司拥有CCRC风险评估二级、CCRC安全集成二级、ISO27001、CMMI-5等21项企业资质，业务涵盖网信安全、云计算、大数据、物联网、聚翼平台、DICT平台、智慧化行业应用及电信资源提供、运营维护等，专注于行业客户ICT服务支撑。深耕市场多年，拥有丰富的ICT项目服务经验，积累了包括政务、金融、教育等行业的上百个优秀案例，打造了众多标杆项目。

入会联系人：张玉萍　　联系电话：027-82757716

入会通道：https://www.whcsa.org.cn/public/portal/list/index/id/11.html

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及专业人士，我会诚邀您加入到“武汉网络安全”的大家庭中来，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！

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 人员培训

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

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/public/portal/list/index/id/11.html