武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2023年第2期　总第2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。

协会是中国网络社会组织联合会和中国网络空间安全协会成员单位、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”；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；成立了华中第一个智能汽车网络安全专业委员会，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。

协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

尊敬的各位理事、会员、读者：

当前，人类社会正加速迈向数字文明时代，伴随数字化、网络化、智能化深入发展，国家安全的内涵和外延更加丰富，时空领域更加宽广，内外因素更加复杂。网络安全与政治安全、经济安全、文化安全、社会安全、军事安全等领域相互交融、相互影响，已成为我国面临的最复杂、最现实、最严峻的非传统安全问题之一，在国家安全体系中的基础性、战略性、全局性地位更加凸显。

党的十八大以来，以习近平同志为核心的党中央深刻洞察和准确把握国家安全形势变化新特点，统筹发展和安全，对我国网络安全工作作出一系列新部署新要求。在习近平总书记关于网络强国的重要思想指引下，我国网络安全体系建设不断完善，网络安全保障能力持续提升，网络安全技术和产业蓬勃发展，网络安全防线全方位巩固，有力护航网络强国、数字中国乘风破浪、行稳致远。

武汉市网络安全协会作为我市网络安全产业的代表，在市委网信办的指导和支持下，持续协助各级主管部门推进武汉市网络安全产业教育融合发展工作，协助市委网信办组织了多场全市网络安全培训，持续参与组织国家网络安全宣传周活动，主办协办各项赛事和论坛活动，积极推进各专业委员会的组建，启动了多项重要领域网络安全团体标准编制工作，将网安工作触角深入到了我市各行各业，为保障我市关键信息基础设施安全，强化网络安全保障，不断提升城市安全保障水平和安全发展能力做出了积极贡献。

作为武汉市网络安全协会专家委员会的主任，我非常荣幸能够通过协会这个交流合作的平台与各位协会成员和行业专家共同探讨网络安全的专业议题，共同从事网络安全工作。

专家委员会将继续发扬科技学术民主精神，团结全市网络安全领域的科技工作者和技术骨干，推动我市网络安全行业的科技创新和技术进步，促进网络安全人才队伍成长，广泛开展网络安全技术交流活动，共同为我市网络安全技术和产业发展，发挥专业智库作用、实现集体价值。

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、二级教授、博士生导师）

目 录

CATALOGUE

公约倡议

协会动态

新增会员

湖北省人民政府办公厅关于印发湖北省数字经济高质量发展若干政策措施的通知

各市、州、县人民政府，省政府各部门：

《湖北省数字经济高质量发展若干政策措施》已经省政府同意，现印发给你们，请认真贯彻执行。

2023 年 5 月 5 日

湖北省数字经济高质量发展若干政策措施

为深入学习贯彻党的二十大精神和习近平总书记关于数字经济发展的重要论述，落实省第十二次党代会关于打造全国数字经济发展高地的决策部署，加快推进全省数字经济高质量发展，制定以下政策措施。

一、加快新型基础设施建设

1．加快 5G 网络建设。支持以 5G 为代表的“双千兆”网络建设。2023 年至 2025 年对电信服务企业新建 5G 宏基站超出上一年度总数的部分给予奖励，按每个 5G 宏基站 1 万元进行奖补，力争 5G 基站数量继续保持中部领先、全国靠前。（责任单位：省经信厅、省通信管理局、省财政厅，各市、州人民政府）

2．加快创新基础设施建设布局。积极争取国家数字经济重大基础设施、国家级研究院等平台载体落户湖北。加快国家网络安全人才与创新基地、国家工业互联网标识解析（武汉）顶级节点、城市数字公共基础设施国家试点、国家新型互联网交换中心试点建设，对相应的国家重大基础设施建设项目，采取“一事一议”的方式予以支持，每个项目一次性补助最高不超过 500 万元。对在北斗、量子网络、新型数据中心、人工智能计算中心、高性能计算等领域，新建且投入超过 2 亿元以上的创新基础设施，择优按资金投入一定比例给予建设和运营经费补贴，每个最高不超过 500 万元。对省内新建的工业互联网二级节点、区块链骨干节点，按资金投入 10% 给予一次性运营经费补贴，每个最高不超过 200 万元。（责任单位：省经信厅、省通信管理局、省发改委、省广电局、省财政厅，各市、州、县人民政府）

二、大力提升数字经济核心产业能级

3．招引培育数字经济龙头企业。对总部（含研发总部和区域总部）新落户我省的全国电子信息企业竞争力百强（中国电子信息行业联合会发布）、软件和信息技术服务竞争力百强（中国电子信息行业联合会发布）、中国互联网企业百强（中国互联网协会发布）榜单企业，且投资达到 5000 万元以上或网络零售首次达到 50 亿元以上的给予一次性奖补 500 万元，对首次进入上述榜单的省内企业，给予一次性奖补 500 万元。（责任单位：省经信厅、省发改委、省商务厅、省财政厅）

4．加快推进企业做大做强。加快培育省内电子信息制造、软件和信息服务、人工智能和大数据等数字

经济核心产业企业做大做强，坚持产业链高质量发展“链长＋链主＋链创”三链机制，按统计数据对电子信息制造企业主营业务收入、软件企业软件业务收入首次突破 20 亿元、30 亿元的，分别给予 30 万元、50 万元一次性奖励。（责任单位：省经信厅、省财政厅）

5．推动大中小企业融通发展。发挥产业链链主企业引领支撑作用，推动产业链上下游协同发展。支持省内龙头骨干企业打造行业级、区域级或跨行业、跨领域工业互联网平台，引导中小微企业上云上平台，降低企业数字化成本，提升企业数字化转型能力和水平。（责任单位：省经信厅，各市、州、县人民政府）

6．促进产业集聚发展。推进武汉“中国软件特色名城”提档升级，加快打造“电竞之城”。支持国家区块链发展先导区、人工智能创新应用先导区、工业互联网产业示范基地、“5G+ 工业互联网”融合应用先导区和工业互联网数字化转型促进中心等加快建设，培育各具特色的数字经济示范园区。探索园区考评机制，支持在全省范围内打造一批标杆数字经济园区，建立以 5G 网络覆盖、工业互联网平台应用、人工智能、企业上云、信息安全等为导向的园区综合评价机制，对绩效评价靠前的分档次给予最高 500 万元奖励。奖补资金由园区运营主体统筹安排用于补贴园区内企业电费、宽带资费、数据资费、算力资费、场地租金等费用。（责任单位：省发改委、省经信厅、省财政厅、省通信管理局）

三、推进数字经济与实体经济深度融合

7．支持国家级数字经济融合应用示范。对省内企业新认定的国家级数字经济领域优秀产品、试点示范项目（含标杆、优秀案例、揭榜挂帅等），一次性奖励 50 万元，对获批的国家“数字领航”企业，再奖补 200 万元。对省内企业首次获评国家级“双跨”工业互联网平台的，每个一次性奖补 500 万元。对首次通过国家两化融合管理体系 3A 级认定的工业企业一次性补助 50 万元；支持企业开展数据管理成熟度模型（DCMM）贯标，对首次通过 DCMM 贯标 2 级以上的企业，分别给予最高不超过 50 万元的奖补。（责任单位：省经信厅、省财政厅、省通信管理局）

8．深化新一代信息技术与制造业融合应用。围绕工业领域网络化、数字化、智能化改造升级，每年面向省内工业企业、软件和信息服务业企业发放上云服务券，分级分类对购买云服务企业给予采购费用补贴。持续开展省级两化融合试点示范企业、上云标杆、信

息消费、工业互联网平台（含“双跨”工业互联网平台）、5G 全连接工厂评选，对新增省级 5G 全连接工厂每个一次性给予 30 万元奖补，省级“双跨”工业互联网平台每个一次性奖补 100 万元。有条件的市（州）应出台政策对省级数字经济相关试点示范、标杆、优秀案例进行奖补。（责任单位：省经信厅、省财政厅、省通信管理局，各市、州人民政府）

9．支持数字经济项目建设。支持云计算、大数据、人工智能、工业互联网、区块链、元宇宙、数据安全等新一代信息技术在各领域的应用，建立省级数字经济项目库，择优遴选总投资 1000 万元以上的新开工数字经济项目，按照项目软硬件投资额的 8% 给予支持，单个项目补助金额不超过 500 万元。（责任单位：省经信厅、省财政厅、省数字经济联席会议各成员单位，各市、州人民政府）

10．大力培育应用场景。支持新业态、新模式在一、二、三产业的融合应用，对开放各类资源、面向公众建立创新、创业、服务的应用场景，每年遴选 100 个优秀应用场景进行宣传推广，并择优给予项目建设主体 50 万元的一次性奖补。鼓励各市（州）围绕数字经济、工业互联网、信息消费等建设展厅、体验中心等，按照项目建设实际投入的 20% 给予补贴，每个最高不超过 200 万元。（责任单位：省经信厅、省数字经济联席会议各成员单位）

四、大力开展关键技术创新及应用

11．加快数字经济创新成果转化。探索建立动态调整的省级数字经济核心领域首台（套）装备、首批次新材料、首版次软件（以下简称“三首”）奖补目录，对省内注册经评定的首台（套）、首批次产品省内研制单位和示范应用单位，分别按照单价的 15% 给予省内研制单位和示范应用单位一次性奖补，双边奖补合计最高 1000 万元。对首版次软件按照研发成本的 15% 给予省内研制单位一次性奖补，按照单价的 50% 给予省内示范应用单位一次性奖补，双边奖补合计最高 1000 万元。鼓励银行业金融机构加大对企业研制“三首”产品的信贷支持力度，加大政策性融资担保支持，引导融资租赁公司做好对“三首”产品推广应用的融资服务。（责任单位：省经信厅、省金融监管局、省财政厅）

12．支持数字经济企业技术攻关。鼓励省内企业联合科研院所面向未来产业，开展 6G、量子科技、人形机器人、元宇宙、人工智能等领域原创性研发，对相关企业享受研发费用加计扣除超出上一年度的增量部分给予补助，单家企业补助额最高可达 100 万元；鼓励市县加大投入，地方财政科技投入增幅超出全省平均水平的，所在地企业可适当上浮奖励系数。对总部设在湖北并从事关键软件独立研发的企业，对年度研发投入超出 1000 万元的，超出部分按 5% 比例给予一次性补贴，每家企业每年最高补贴 500 万元。（责任单位：省财政厅、省科技厅、省经信厅）

五、营造良好发展环境

13．强化统筹推进。发挥省数字经济联席会议统筹协调作用，形成省直部门横向协同，省、市（州）、县（市、区）纵向联动的工作机制，包容审慎对待数字经济新业态、新模式。省财政通过省级数字经济高质量发展专项，对资金统筹投入力度大、工作成效显著的相关部门给予奖补配套支持。（责任单位：省经信厅、省财政厅、省发改委、省市场监管局，各市、州、县人民政府）

14．加大财税金融支持。充分发挥总规模 100 亿元的省数字经济产业基金作用，引导社会资本投资数字经济领域重大项目，拓宽数字经济市场主体融资渠道。鼓励有条件的市（州）设立数字经济专项资金。（责任单位：省经信厅、省金融监管局，长江产业投资集团，各市、州、县人民政府）

15．加强监测评估。建立健全数字经济统计监测制度，组织对各市（州）开展年度综合评价，发布全省数字经济工作动态、数字经济白皮书，定期分析研判数字经济发展态势。对年度推进数字经济发展成效显著的市县给予督查激励。（责任单位：省经信厅、省发改委、省统计局、省市场监管局，各市、州、县人民政府）

李强签国务院令 公布修订后的《商用密码管理条例》

中华人民共和国国务院令

第760号

《商用密码管理条例》已经 2023 年 4 月 14 日国务院第 4 次常务会议修订通过，现予公布，自 2023 年 7 月 1 日起施行。

总理 李强

2023 年 4 月 27 日

商用密码管理条例

（1999 年 10 月 7 日中华人民共和国国务院令第 273 号发布 2023 年 4 月 27 日中华人民共和国国务院令第 760 号修订）

第一章 总则

第一条 为了规范商用密码应用和管理，鼓励和促进商用密码产业发展，保障网络与信息安全，维护国家安全和社会公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国密码法》等法律，制定本条例。

第二条 在中华人民共和国境内的商用密码科研、生产、销售、服务、检测、认证、进出口、应用等活动及监督管理，适用本条例。

本条例所称商用密码，是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。

第三条 坚持中国共产党对商用密码工作的领导，贯彻落实总体国家安全观。国家密码管理部门负责管理全国的商用密码工作。县级以上地方各级密码管理部门负责管理本行政区域的商用密码工作。

网信、商务、海关、市场监督管理等有关部门在各自职责范围内负责商用密码有关管理工作。

第四条 国家加强商用密码人才培养，建立健全商用密码人才发展体制机制和人才评价制度，鼓励和支持密码相关学科和专业建设，规范商用密码社会化培训，促进商用密码人才交流。

第五条 各级人民政府及其有关部门应当采取多种形式加强商用密码宣传教育，增强公民、法人和其他组织的密码安全意识。

第六条 商用密码领域的学会、行业协会等社会组织依照法律、行政法规及其章程的规定，开展学术交流、政策研究、公共服务等活动，加强学术和行业自律，推动诚信建设，促进行业健康发展。

密码管理部门应当加强对商用密码领域社会组织的指导和支持。

第二章 科技创新与标准化

第七条 国家建立健全商用密码科学技术创新促进机制，支持商用密码科学技术自主创新，对作出突出贡献的组织和个人按照国家有关规定予以表彰和奖励。

国家依法保护商用密码领域的知识产权。从事商用密码活动，应当增强知识产权意识，提高运用、保护和管理知识产权的能力。

国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术。

第八条 国家鼓励和支持商用密码科学技术成果转化和产业化应用，建立和完善商用密码科学技术成果信息汇交、发布和应用情况反馈机制。

第九条 国家密码管理部门组织对法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统所使用的密码算法、密码协议、密钥管理机制等商用密码技术进行审查鉴定。

第十条 国务院标准化行政主管部门和国家密码管理部门依据各自职责，组织制定商用密码国家标准、行业标准，对商用密码团体标准的制定进行规范、引导和监督。国家密码管理部门依据职责，建立商用密码标准实施信息反馈和评估机制，对商用密码标准实施进行监督检查。

国家推动参与商用密码国际标准化活动，参与制定商用密码国际标准，推进商用密码中国标准与国外标准之间的转化运用，鼓励企业、社会团体和教育、科研机构等参与商用密码国际标准化活动。

其他领域的标准涉及商用密码的，应当与商用密码国家标准、行业标准保持协调。

第十一条 从事商用密码活动，应当符合有关法律、行政法规、商用密码强制性国家标准，以及自我声明公开标准的技术要求。

国家鼓励在商用密码活动中采用商用密码推荐性国家标准、行业标准，提升商用密码的防护能力，维护用户的合法权益。

第三章 检测认证

第十二条 国家推进商用密码检测认证体系建设，鼓励在商用密码活动中自愿接受商用密码检测认证。

第十三条 从事商用密码产品检测、网络与信息系统商用密码应用安全性评估等商用密码检测活动，向社会出具具有证明作用的数据、结果的机构，应当经国家密码管理部门认定，依法取得商用密码检测机构资质。

第十四条 取得商用密码检测机构资质，应当符合下列条件：

（一）具有法人资格；

（二）具有与从事商用密码检测活动相适应的资金、场所、设备设施、专业人员和专业能力；

（三）具有保证商用密码检测活动有效运行的管理体系。

第十五条 申请商用密码检测机构资质，应当向国家密码管理部门提出书面申请，并提交符合本条例第十四条规定条件的材料。

国家密码管理部门应当自受理申请之日起 20 个工作日内，对申请进行审查，并依法作出是否准予认定的决定。

需要对申请人进行技术评审的，技术评审所需时间不计算在本条规定的期限内。国家密码管理部门应当将所需时间书面告知申请人。

第十六条 商用密码检测机构应当按照法律、行政法规和商用密码检测技术规范、规则，在批准范围内独立、公正、科学、诚信地开展商用密码检测，对出具的检测数据、结果负责，并定期向国家密码管理部门报送检测实施情况。

商用密码检测技术规范、规则由国家密码管理部门制定并公布。

第十七条 国务院市场监督管理部门会同国家密码管理部门建立国家统一推行的商用密码认证制度，实行商用密码产品、服务、管理体系认证，制定并公布认证目录和技术规范、规则。

第十八条 从事商用密码认证活动的机构，应当依法取得商用密码认证机构资质。

申请商用密码认证机构资质，应当向国务院市场监督管理部门提出书面申请。申请人除应当符合法律、行政法规和国家有关规定要求的认证机构基本条件外，还应当具有与从事商用密码认证活动相适应的检测、检查等技术能力。

国务院市场监督管理部门在审查商用密码认证机构资质申请时，应当征求国家密码管理部门的意见。

第十九条 商用密码认证机构应当按照法律、行政法规和商用密码认证技术规范、规则，在批准范围内独立、公正、科学、诚信地开展商用密码认证，对出具的认证结论负责。

商用密码认证机构应当对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查，以保证通过认证的商用密码产品、服务、管理体系持续符合认证要求。

第二十条 涉及国家安全、国计民生、社会公共利益的商用密码产品，应当依法列入网络关键设备和网络安全专用产品目录，由具备资格的商用密码检测、认证机构检测认证合格后，方可销售或者提供。

第二十一条 商用密码服务使用网络关键设备和网络安全专用产品的，应当经商用密码认证机构对该商用密码服务认证合格。

第四章 电子认证

第二十二条 采用商用密码技术提供电子认证服务，应当具有与使用密码相适应的场所、设备设施、专业人员、专业能力和管理体系，依法取得国家密码管理部门同意使用密码的证明文件。

第二十三条 电子认证服务机构应当按照法律、行政法规和电子认证服务密码使用技术规范、规则，使用密码提供电子认证服务，保证其电子认证服务密码使用持续符合要求。

电子认证服务密码使用技术规范、规则由国家密码管理部门制定并公布。

第二十四条 采用商用密码技术从事电子政务电子认证服务的机构，应当经国家密码管理部门认定，依法取得电子政务电子认证服务机构资质。

第二十五条 取得电子政务电子认证服务机构资质，应当符合下列条件：

（一）具有企业法人或者事业单位法人资格；

（二）具有与从事电子政务电子认证服务活动及其使用密码相适应的资金、场所、设备设施和专业人员；

（三）具有为政务活动提供长期电子政务电子认证服务的能力；

（四）具有保证电子政务电子认证服务活动及其使用密码安全运行的管理体系。

第二十六条 申请电子政务电子认证服务机构资质，应当向国家密码管理部门提出书面申请，并提交符合本条例第二十五条规定条件的材料。

国家密码管理部门应当自受理申请之日起 20 个工作日内，对申请进行审查，并依法作出是否准予认定的决定。

需要对申请人进行技术评审的，技术评审所需时间不计算在本条规定的期限内。国家密码管理部门应当将所需时间书面告知申请人。

第二十七条 外商投资电子政务电子认证服务，影响或者可能影响国家安全的，应当依法进行外商投资安全审查。

第二十八条 电子政务电子认证服务机构应当按照法律、行政法规和电子政务电子认证服务技术规范、规则，在批准范围内提供电子政务电子认证服务，并定期向主要办事机构所在地省、自治区、直辖市密码管理部门报送服务实施情况。

电子政务电子认证服务技术规范、规则由国家密码管理部门制定并公布。

第二十九条 国家建立统一的电子认证信任机制。国家密码管理部门负责电子认证信任源的规划和管理，会同有关部门推动电子认证服务互信互认。

第三十条 密码管理部门会同有关部门负责政务活动中使用电子签名、数据电文的管理。

政务活动中电子签名、电子印章、电子证照等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。

第五章 进出口

第三十一条 涉及国家安全、社会公共利益且具有加密保护功能的商用密码，列入商用密码进口许可清单，实施进口许可。涉及国家安全、社会公共利益或者中国承担国际义务的商用密码，列入商用密码出口管制清单，实施出口管制。

商用密码进口许可清单和商用密码出口管制清单由国务院商务主管部门会同国家密码管理部门和海关总署制定并公布。

大众消费类产品所采用的商用密码不实行进口许可和出口管制制度。

第三十二条 进口商用密码进口许可清单中的商用密码或者出口商用密码出口管制清单中的商用密码，应当向国务院商务主管部门申请领取进出口许可证。

商用密码的过境、转运、通运、再出口，在境外与综合保税区等海关特殊监管区域之间进出，或者在境外与出口监管仓库、保税物流中心等保税监管场所之间进出的，适用前款规定。

第三十三条 进口商用密码进口许可清单中的商用密码或者出口商用密码出口管制清单中的商用密码时，应当向海关交验进出口许可证，并按照国家有关规定办理报关手续。

进出口经营者未向海关交验进出口许可证，海关有证据表明进出口产品可能属于商用密码进口许可清单或者出口管制清单范围的，应当向进出口经营者提出质疑；海关可以向国务院商务主管部门提出组织鉴别，并根据国务院商务主管部门会同国家密码管理部门作出的鉴别结论依法处置。在鉴别或者质疑期间，海关对进出口产品不予放行。

第三十四条 申请商用密码进出口许可，应当向国务院商务主管部门提出书面申请，并提交下列材料：

（一）申请人的法定代表人、主要经营管理人以及经办人的身份证明；

（二）合同或者协议的副本；

（三）商用密码的技术说明；

（四）最终用户和最终用途证明；

（五）国务院商务主管部门规定提交的其他文件。

国务院商务主管部门应当自受理申请之日起 45 个工作日内，会同国家密码管理部门对申请进行审查，并依法作出是否准予许可的决定。

对国家安全、社会公共利益或者外交政策有重大影响的商用密码出口，由国务院商务主管部门会同国

家密码管理部门等有关部门报国务院批准。报国务院批准的，不受前款规定时限的限制。

第六章 应用促进

第三十五条 国家鼓励公民、法人和其他组织依法使用商用密码保护网络与信息安全，鼓励使用经检测认证合格的商用密码。

任何组织或者个人不得窃取他人加密保护的信息或者非法侵入他人的商用密码保障系统，不得利用商用密码从事危害国家安全、社会公共利益、他人合法权益等违法犯罪活动。

第三十六条 国家支持网络产品和服务使用商用密码提升安全性，支持并规范商用密码在信息领域新技术、新业态、新模式中的应用。

第三十七条 国家建立商用密码应用促进协调机制，加强对商用密码应用的统筹指导。国家机关和涉及商用密码工作的单位在其职责范围内负责本机关、本单位或者本系统的商用密码应用和安全保障工作。

密码管理部门会同有关部门加强商用密码应用信息收集、风险评估、信息通报和重大事项会商，并加强与网络安全监测预警和信息通报的衔接。

第三十八条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，自行或者委托商用密码检测机构开展商用密码应用安全性评估。

前款所列关键信息基础设施通过商用密码应用安全性评估方可投入运行，运行后每年至少进行一次评估，评估情况按照国家有关规定报送国家密码管理部门或者关键信息基础设施所在地省、自治区、直辖市密码管理部门备案。

第三十九条 法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。

第四十条 关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

第四十一条 网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。

第四十二条 商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。

第七章 监督管理

第四十三条 密码管理部门依法组织对商用密码活动进行监督检查，对国家机关和涉及商用密码工作的单位的商用密码相关工作进行指导和监督。

第四十四条 密码管理部门和有关部门建立商用密码监督管理协作机制，加强商用密码监督、检查、指导等工作的协调配合。

第四十五条 密码管理部门和有关部门依法开展商用密码监督检查，可以行使下列职权：

（一）进入商用密码活动场所实施现场检查；

（二）向当事人的法定代表人、主要负责人和其他有关人员调查、了解有关情况；

（三）查阅、复制有关合同、票据、账簿以及其他有关资料。

第四十六条 密码管理部门和有关部门推进商用密码监督管理与社会信用体系相衔接，依法建立推行商用密码经营主体信用记录、信用分级分类监管、失信惩戒以及信用修复等机制。

第四十七条 商用密码检测、认证机构和电子政务电子认证服务机构及其工作人员，应当对其在商用密码活动中所知悉的国家秘密和商业秘密承担保密义务。

密码管理部门和有关部门及其工作人员不得要求

商用密码科研、生产、销售、服务、进出口等单位和商用密码检测、认证机构向其披露源代码等密码相关专有信息，并对其在履行职责中知悉的商业秘密和个人隐私严格保密，不得泄露或者非法向他人提供。

第四十八条 密码管理部门和有关部门依法开展商用密码监督管理，相关单位和人员应当予以配合，任何单位和个人不得非法干预和阻挠。

第四十九条 任何单位或者个人有权向密码管理部门和有关部门举报违反本条例的行为。密码管理部门和有关部门接到举报，应当及时核实、处理，并为举报人保密。

第八章 法律责任

第五十条 违反本条例规定，未经认定向社会开展商用密码检测活动，或者未经认定从事电子政务电子认证服务的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款。

违反本条例规定，未经批准从事商用密码认证活动的，由市场监督管理部门会同密码管理部门依照前款规定予以处罚。

第五十一条 商用密码检测机构开展商用密码检测，有下列情形之一的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销商用密码检测机构资质：

（一）超出批准范围；

（二）存在影响检测独立、公正、诚信的行为；

（三）出具的检测数据、结果虚假或者失实；

（四）拒不报送或者不如实报送实施情况；

（五）未履行保密义务；

（六）其他违反法律、行政法规和商用密码检测技术规范、规则开展商用密码检测的情形。

第五十二条 商用密码认证机构开展商用密码认证，有下列情形之一的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销商用密码认证机构资质：

（一）超出批准范围；

（二）存在影响认证独立、公正、诚信的行为；

（三）出具的认证结论虚假或者失实；

（四）未对其认证的商用密码产品、服务、管理体系实施有效的跟踪调查；

（五）未履行保密义务；

（六）其他违反法律、行政法规和商用密码认证技术规范、规则开展商用密码认证的情形。

第五十三条 违反本条例第二十条、第二十一条规定，销售或者提供未经检测认证或者检测认证不合格的商用密码产品，或者提供未经认证或者认证不合格的商用密码服务的，由市场监督管理部门会同密码管理部门责令改正或者停止违法行为，给予警告，没收违法产品和违法所得；违法所得 10 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 10 万元的，可以并处 3 万元以上 10 万元以下罚款。

第五十四条 电子认证服务机构违反法律、行政法规和电子认证服务密码使用技术规范、规则使用密码的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，依法吊销电子认证服务使用密码的证明文件。

第五十五条 电子政务电子认证服务机构开展电子政务电子认证服务，有下列情形之一的，由密码管理部门责令改正或者停止违法行为，给予警告，没收违

法所得；违法所得 30 万元以上的，可以并处违法所得 1 倍以上 3 倍以下罚款；没有违法所得或者违法所得不足 30 万元的，可以并处 10 万元以上 30 万元以下罚款；情节严重的，责令停业整顿，直至吊销电子政务电子认证服务机构资质：

（一）超出批准范围；

（二）拒不报送或者不如实报送实施情况；

（三）未履行保密义务；

（四）其他违反法律、行政法规和电子政务电子认证服务技术规范、规则提供电子政务电子认证服务的情形。

第五十六条 电子签名人或者电子签名依赖方因依据电子政务电子认证服务机构提供的电子签名认证服务在政务活动中遭受损失，电子政务电子认证服务机构不能证明自己无过错的，承担赔偿责任。

第五十七条 政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务，违反本条例第三十条规定，未由依法设立的电子政务电子认证服务机构提供的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，由密码管理部门建议有关国家机关、单位对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关、单位应当将处分或者处理情况书面告知密码管理部门。

第五十八条 违反本条例规定进出口商用密码的，由国务院商务主管部门或者海关依法予以处罚。

第五十九条 窃取他人加密保护的信息，非法侵入他人的商用密码保障系统，或者利用商用密码从事危害国家安全、社会公共利益、他人合法权益等违法活动的，由有关部门依照《中华人民共和国网络安全法》和其他有关法律、行政法规的规定追究法律责任。

第六十条 关键信息基础设施的运营者违反本条例第三十八条、第三十九条规定，未按照要求使用商用密码，或者未按照要求开展商用密码应用安全性评估的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款。

第六十一条 关键信息基础设施的运营者违反本条例第四十条规定，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额 1 倍以上 10 倍以下罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第六十二条 网络运营者违反本条例第四十一条规定，未按照国家网络安全等级保护制度要求使用商用密码保护网络安全的，由密码管理部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处 1 万元以上 10 万元以下罚款，对直接负责的主管人员处 5000 元以上 5 万元以下罚款。

第六十三条 无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节特别严重的，责令停业整顿，直至吊销商用密码许可证件。

第六十四条 国家机关有本条例第六十条、第六十一条、第六十二条、第六十三条所列违法情形的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，由密码管理部门、有关部门建议有关国家机关对直接负责的主管人员和其他直接责任人员依法给予处分或者处理。有关国家机关应当将处分或者处理情况书面告知密码管理部门、有关部门。

第六十五条 密码管理部门和有关部门的工作人员在商用密码工作中滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第六十六条 违反本条例规定，构成犯罪的，依法追究刑事责任；给他人造成损害的，依法承担民事责任。

第九章 附则

第六十七条 本条例自 2023 年 7 月 1 日起施行。

湖北省数字经济促进办法

湖北省人民政府令第 427 号

《湖北省数字经济促进办法》已经 2023 年 3 月 2 日省人民政府第 6 次常务会议审议通过，现予公布，自 2023 年 7 月 1 日起施行。

省长 王忠林

2023 年 5 月 10 日

湖北省数字经济促进办法

第一章 总则

第一条 为了加快发展数字经济，推进数字产业化、产业数字化，推动数据要素资源高效流通使用，促进数字经济和实体经济深度融合，打造全国数字经济发展高地，根据有关法律、法规，结合本省实际，制定本办法。

第二条 本办法适用于本省行政区域内数字基础设施建设、数字产业化、产业数字化、数据资源开发利用保护和数字技术创新等相关活动。

本办法所称数字经济，是指以数据资源为关键要素，以现代信息网络为主要载体，以信息通信技术融合应用、全要素数字化转型为重要推动力，促进公平与效率更加统一的新经济形态。

第三条 发展数字经济应当坚持数据赋能、突出优势、市场主导、包容审慎，推动数字经济创新、协同、开放、安全发展。

第四条 省人民政府加强对全省数字经济发展的统一领导，健全数字经济协调机制，统筹协调全省数字经济发展工作，研究制定数字经济发展重大政策，营造数字经济发展良好环境。

县级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划，根据需要制定本地区数字经济发展规划，建立数字经济协调机制，完善数字经济发展政策，支持开展数字技术创新和应用，促进数字经济健康发展。

第五条 省人民政府数据主管部门负责统筹推进数字经济发展，协调推进数据要素制度建设，统筹数据资源整合共享和开发利用，推进数字基础设施布局建设等。

省人民政府发展改革部门负责拟定促进数字经济发展战略、规划和重大政策，推进数字经济发展重大工程和项目实施等。

省人民政府经济和信息化主管部门负责推进数字产业化发展、产业数字化转型等。

省人民政府科学技术行政部门负责指导、协调数字经济创新平台建设，推动数字技术基础研究、关键核心技术攻关和科技成果转化。

省人民政府统计部门负责建立数字经济统计监测制度，开展数字经济统计调查和监测分析。

省人民政府政务主管部门负责公共数据管理，组织协调公共数据归集、共享、开放及安全管理等工作。

省网络安全和信息化主管部门统筹协调网络安全、数据安全、个人信息保护及相关监督管理等工作。

省人民政府其他有关部门按照职责分工依法做好促进数字经济发展有关工作。

设区的市、自治州和县级人民政府确定的数字经济主管部门负责推进本地区数字经济发展工作。

第六条 省人民政府及其有关部门应当结合落实“数字丝绸之路”建设、中部地区崛起、长江经济带发展等国家重大战略，发挥长江中游城市群省际协商合作机制作用，促进重大数字基础设施共建共享、数据标准统一规范、数据资源共享开放、数据资产价值评估、数字技术协同创新等。鼓励中国（湖北）自由贸易试验区探索数据跨境安全有序流动。

县级以上人民政府应当按照本省区域发展布局，加强数字经济跨区域合作和政策协调，共同促进数字经济发展。

支持举办数字经济领域的交流活动，充分利用数字经济展示交易、交流合作平台，加强数字经济领域国际合作交流。

第七条 县级以上人民政府及有关部门应当开展数字经济领域的知识、技术技能、法律法规等宣传，开展数字技能教育和培训，提升公民数字素养。

第八条 鼓励和支持各类市场主体参与数字经济基础设施建设、产业发展、数字化转型、科技创新、数据开发利用保护等活动。

鼓励和支持高等学校、科研机构、学术团体、行业协会、产业联盟、新型智库等为促进数字经济发展提供人才培养、创业孵化、投资融资、技术支持、产权交易等服务。

第二章 数字基础设施建设

第九条 省人民政府应当完善数字基础设施发展布局，统筹各级人民政府及其相关部门推动建设网络基础设施、算力基础设施、融合基础设施，推进传统基础设施的数字化改造，促进数字基础设施互联互通、共建共享、集约利用。

第十条 数字基础设施布局建设应当符合国土空间规划。市政、交通、电力、燃气、公共安全等相关基础设施规划应当适应数字经济发展需要，与数字基础设施相关规划相互协调和衔接。

第十一条 县级以上人民政府及其有关部门应当加快网络基础设施建设，支持建设新一代移动通信技术网络和高速固定宽带网络，推进城乡信息通信网络服务能力一体化，提升网络性能和服务能力；推动网络基础设施与公路、铁路、城市轨道、桥梁、隧道、电力、地下综合管廊、机场、港口等基础设施以及相关配套设施共建共享。

公共机构以及公共场所、公共设施的所有者、管理者应当支持网络基础设施建设，按照国家和本省有关规定开放建筑物、绿地、杆塔等资源，推进智慧杆塔建设和一杆多用。

鼓励有条件的地区建设泛在互联、智能感知的物联网，推进基础设施、物流仓储、生产制造、生活服务、生态环境保护、应急管理等领域感知系统的建设应用、互联互通和数据共享。

第十二条 省人民政府及其发展改革、数据、科学技术、经济和信息化等主管部门以及通信管理部门应当按照全国一体化大数据中心总体布局推进算力基础设施建设，推动通用数据中心、超级计算中心、智能计算中心、边缘数据中心等合理布局，统筹推进人工智能、区块链、云计算等基础设施建设，支持建设底层技术平台、算法平台、开源平台等基础平台，建立通用技术能力支撑体系。

省、设区的市、自治州人民政府及其有关部门应当推动既有数据中心节能改造，支持数据中心提升可再生能源电力消费比重，支持数据中心集群配套可再

生能源电站。

第十三条 县级以上人民政府应当推进工业、农业、能源、水利、城建、医疗、教育、文旅等重点行业融合基础设施建设，对传统基础设施进行数字化、智能化改造，加快新型城市基础设施建设，增强数据感知、边缘计算和智能分析能力。

第三章 数字产业化

第十四条 县级以上人民政府应当根据数字技术和产业发展趋势，结合本地区数字产业发展水平和资源禀赋，围绕数字经济核心产业，通过延伸创新链、完善产业链、保障供应链安全、培育产业集群等方式，促进产业协同和供应保障，提高数字产业整体竞争力。

第十五条 县级以上人民政府及其有关部门根据全省数字经济发展规划，结合本地区实际，通过规划引导、政策支持、市场主体培育等方式，重点发展下列数字产业集群：

（一）光电子信息；

（二）集成电路；

（三）新型显示；

（四）智能终端；

（五）信息通信；

（六）软件信息服务；

（七）数字算力及存储；

（八）北斗；

（九）信息安全；

（十）其他重要数字产业集群。

积极培育区块链、人工智能、信息技术应用创新等新兴数字产业，前瞻布局类脑智能、量子信息、下一代移动通信、元宇宙等未来产业。

第十六条 县级以上人民政府及其经济和信息化、发展改革、数据、科学技术等主管部门应当支持数字企业发展壮大，丰富数字技术应用场景，建立数字经济企业储备库，吸引数字经济龙头企业在本省设立主要办事机构或者大型分支机构，培育数字产业高新技术企业，鼓励专业化、精细化、特色化、新颖化中小企业发展。

第十七条 县级以上人民政府及其发展改革、数据、经济和信息化、商务、市场监督管理等主管部门应当推进平台经济、共享经济等规范健康持续发展，督促平台企业建立健全平台管理制度规则，促进各类平台融合互通；支持企业建设生产服务、生活服务等互联网平台，引导平台企业建立数据开放机制。鼓励企业探索建立共享设备、共享车间、共享工厂、共享科技资源、共享物流等共享经济新型组织模式。

平台企业应当遵守法律法规、商业道德，不得利用数据、算法、流量、市场、资本优势，排除或者限制其他平台和应用独立运行，不得损害中小企业合法权益，不得对消费者实施不公平的差别待遇和选择限制。

第十八条 引导互联网企业、行业龙头企业、基础电信业务经营者开放数据资源和平台计算能力等；支持企业、高等学校、科研机构等创建数字经济领域众创空间、科技企业孵化器、科技企业加速器、大学科技园等创新创业载体，构建协同共生的数字经济产业创新生态。

第四章 产业数字化

第十九条 县级以上人民政府及其有关部门应当组织利用数字技术加快推进工业、农业和服务业全方位、全角度、全链条的改造，加快生产模式变革，提高全要素生产率，促进工业、农业和服务业数字化转型发展。

第二十条 县级以上人民政府经济和信息化主管部门应当加速传统产业向智能制造转型，推动关键技术突破，增强工业芯片、工业软件、工业操作系统等供给能力，打造智能车间、智能工厂、数字化产业集群。

县级以上人民政府经济和信息化主管部门应当推动工业企业数字化转型，发展网络化协同制造、个性化定制、远程运维服务、众包众创等新模式，支持大型工业企业开展集成应用创新。

第二十一条 县级以上人民政府经济和信息化主管部门以及通信管理部门应当会同有关部门持续完善工业互联网网络、平台、安全体系，建立健全工业互联

网标识解析体系，加快建设跨领域、跨行业工业互联网平台以及面向重点行业和领域的特色专业型工业互联网平台。

鼓励企业改造提升工业互联网内外网络，推动中小型工业企业运用低成本、快部署、易运维的工业互联网解决方案。支持运用工业互联网整合生产要素，赋能产业集群数字化转型升级。

第二十二条 省人民政府农业农村、乡村振兴等主管部门应当推进数字技术在农业生产各环节的推广应用，建立省级农业农村大数据平台，推动农业数据集成应用，建设农业基础数据资源体系。

县级以上人民政府农业农村、商务、文化和旅游、乡村振兴等主管部门支持农业生产经营主体与互联网企业融合创新，推进农村电商专业化发展，加快农产品流通网络数字化改造，培育“产储运销”一体化发展的荆楚农优品销售模式，打造具有湖北特色的农产品区域公用品牌。鼓励发展创意农业、定制农业、共享农业、云农场、智慧乡村旅游等新业态。

第二十三条 县级以上人民政府发展改革、数据、交通运输、商务等主管部门和邮政管理部门应当推动交通基础设施网、运输服务网、能源网与信息网络建设，支持建设相互融合、物流信息共享和标准互认的物流公共信息服务平台，发展现代物流信息服务，推广无人车、无人机、无人仓等智能化设施设备应用，加强快递末端综合服务站点和设施建设，提升物流全流程数字化、智能化水平。

县级以上人民政府及其经济和信息化、公安、交通运输等主管部门应当支持智能网联汽车依法开展道路测试、商业化运营试点，培育自动驾驶船舶、自动化码头与定制公交、智能公交、智能停车等新业态新模式。

第二十四条 县级以上人民政府及有关部门应当推动数字金融发展，引导和支持数字技术在支付结算、信贷融资、征信服务等金融领域应用，加强数字金融风险隐患排查，完善社会信用体系，提升运行监控和预警能力。

第二十五条 县级以上人民政府商务主管部门应当推进数字技术在商贸流通领域应用，加快商贸流通企业数字化转型，推动线上新型消费加快成长，支持发展直播电商、即时零售等电子商务新业态新模式，引进培育电子商务龙头企业，积极发展“丝路电商”，促进跨境电商发展。

第二十六条 县级以上人民政府文化和旅游主管部门应当会同有关部门加强数字技术在文化、旅游产业的推广应用，发展线上展示与线下体验相结合的服务新模式，加快动漫、电子竞技、数字出版、视频直播等泛娱乐产业快速聚集发展，打造具有荆楚特色的数字文化产品和服务，完善全域智慧文旅综合服务平台功能。

第二十七条 县级以上人民政府教育主管部门应当会同有关部门推动数字技术和教育教学深度融合、创新应用，加快构建数据驱动的人才培养模式和教育治理体系。支持教育数字产业发展，推进教育资源、应用系统、数字化教学设施等各类教育数字化产品的研发和生产，为教育数字化转型提供保障。

第二十八条 县级以上人民政府发展改革、数据、经济和信息化等主管部门统筹建设数字经济产业园区，打造数字化、智能化、绿色化产业集群。

鼓励行业龙头企业建立数字经济产业联盟，推动产业联盟进行全要素、全产业链、全价值链的连接，通过信息、技术、产能、订单共享，实现跨地域、跨行业资源的精准配置与高效对接。

第二十九条 县级以上人民政府经济和信息化、发展改革、数据等主管部门应当完善数字化转型公共服务，培育产业数字化转型服务商，推动建设跨领域、跨行业数字化转型促进中心和配套服务平台，打造区域产业数字化创新综合体，提供产业数字化转型服务。

支持高等学校、科研机构、龙头企业、行业协会等协同合作，建设综合测试验证环境，提供产业共性解决方案。

第五章 数据资源开发利用保护

第三十条 县级以上人民政府及其有关部门应当促

进数据流通使用、依法规范管理、保障数据安全，提升数据资源规模和质量，激活数据要素价值，对公共数据、企业数据和个人数据等实行全生命周期管理，促进数据资源开发保护。

第三十一条 数据收集主体应当按照法律、法规和国家、本省有关规定，采集、管理和维护公共数据、企业数据和个人数据，确保数据真实、准确。

县级以上人民政府及其有关部门应当建立公共数据开放范围动态管理机制，对在依法履行职责、提供服务过程中产生或者获取的公共数据，按照国家和本省的有关规定进行分类分级目录制管理。

县级以上人民政府数据、政务主管部门负责推进公共数据资源统筹管理、整合归集、共享利用，创新公共数据资源开发利用模式和运营机制，规范公共数据产品服务。

第三十二条 县级以上人民政府及其发展改革、数据、经济和信息化、农业农村、商务、市场监督管理、政务等主管部门应当推广使用数据管理相关国家标准和行业标准，规范数据管理，提升数据质量，丰富数据资源。

探索推动企业数据的收集、存储、使用、加工、传输和共享，加强企业数据分类分级管理，支持企业提升数据汇聚、分析、应用能力，鼓励构建数据驱动的生产方式和企业管理模式。

第三十三条 县级以上人民政府及其有关部门应当建立健全高效的公共数据共享协调机制，支持打造公共数据基础支撑平台，推进公共数据归集整合、有序流通和共享。探索完善公共数据共享、开放、运营服务、安全保障的管理体制。优先推进企业登记监管、卫生健康、交通运输、气象等高价值数据向社会开放。探索开展政府数据授权运营。

县级以上人民政府及有关部门应当通过产业政策引导、社会资本引入、应用模式创新、强化合作交流等方式，引导企业等组织、个人依法开放、使用企业数据、个人数据，促进数据融合创新。支持构建工业、农业、服务业等领域数据资源开发利用场景。鼓励依法利用数据开展科学技术研究、咨询服务、产品开发、数据加工等活动。

第三十四条 省人民政府及其有关部门应当根据全国统一大市场建设要求，在保护个人隐私和确保数据

安全的前提下，探索建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制，依法培育数据要素市场，推进数据交易平台建设，逐步建立数据资产评估、登记结算、交易撮合、争议仲裁等市场运营体系，推动数据要素开发利用，发掘数据要素应用场景，提高数据要素配置流通能力。

第三十五条 数据的收集、存储、使用、加工、传输、提供、公开等处理活动，应当遵守法律、法规，履行数据安全保护义务，尊重社会公德和伦理，遵守商业道德和职业道德，诚实守信，承担社会责任。

开展数据处理活动，不得危害国家安全、公共利益，不得损害个人、组织的合法权益。

个人信息受法律保护。个人信息的收集、存储、使用、加工、传输、提供、公开等处理活动，应当遵循合法、正当、必要原则，不得过度处理，并符合法律、法规规定的条件。

第六章 数字技术创新

第三十六条 县级以上人民政府及其有关部门应当推动数字技术创新，加强数字技术基础研究、应用基础研究和技术成果转化，完善产业技术创新体系和共性基础技术供给体系。

第三十七条 省人民政府科学技术行政部门应当会同有关部门组织实施关键核心技术攻关，在光通信、集成电路、新型显示、高端医学影像、大数据、云计算、人工智能、区块链、工业互联网等重点领域，未来网络、量子信息、可见光无线通信、类脑计算等前沿技术领域，加快推进基础理论、基础算法、装备材料等关键核心技术攻关和突破。

省人民政府科学技术行政部门应当会同知识产权等有关部门加快构建国家重大科技项目承接机制，支持在数字技术领域开展高价值专利培育布局，推动获取重大原创科技成果和自主知识产权。

第三十八条 省人民政府及其科学技术、发展改革、数据、经济和信息化等主管部门应当统筹规划、科学布局，加快建设数字经济领域的重点实验室、产业创新中心、技术创新中心、制造业创新中心等创新平台，加强产学研合作，优化科研力量配置和资源共享，促进关键共性技术研发、系统集成和工程化应用，打造数字技术大型综合研究基地和原始创新策源地。

第三十九条 县级以上人民政府及其有关部门应当推动数字技术融合创新，强化企业创新主体地位，支持各类市场主体平等获取数字技术创新资源，推进数字技术创新和产品研发。

鼓励企业与高等学校、科研机构、新型智库开展数字经济产学研合作，共建技术创新联盟、科技创新基地等创新平台。

第四十条 省人民政府经济和信息化主管部门会同发展改革、数据、科学技术、财政等主管部门支持数字技术创新产品和服务的应用推广，将符合条件的数字技术产品和服务认定为首台（套）装备、首批次新材料、首版次软件，列入创新产品目录。

符合条件的，政府采购的采购人经依法批准，可以通过非公开招标方式，采购达到公开招标数额标准的首台（套）装备、首批次新材料、首版次软件。

第七章 保障和监督

第四十一条 县级以上人民政府应当优化服务，在财政、金融、招标投标、人才、知识产权、土地供应、电力接引、能耗指标、设施保护等方面完善政策措施，为促进数字经济发展提供保障。

第四十二条 县级以上人民政府及有关部门应当制定和完善人才政策，加强数字经济领域人才培养、引进、使用、评价、激励、服务。推动数字经济骨干企业与高等学校、科研机构共建人才实训基地，培养复合型、实用型数字经济人才，促进人才供给和市场需求在更大范围内高效匹配。支持高等学校开设数字经济相关学科专业。

逐步建立符合数字经济发展特点的人才评价标准和职业评价体系。数字经济领域引进的高层次、高技能以及紧缺人才应当纳入各级人才支持政策范围，按照规定享受落户、住房、子女教育、配偶就业等服务。

第四十三条 省人民政府统筹保障数字经济发展所需资金，鼓励有条件的设区的市、自治州和县级人民政府在本级财政预算中安排资金，支持数字经济关键核心技术攻关、数字经济核心产业发展、产业数字化转型、数字技术应用场景打造等。

县级以上人民政府应当依法落实数字经济的税收优惠政策，完善投融资服务体系，拓宽数字经济市场主体融资渠道，发挥各级现有投资基金引导作用，重点支持数字经济发展。

鼓励和引导金融机构对符合国家和本省数字经济政策的项目、企业、平台和创新人才，在贷款、政策性融资担保以及其他金融服务等方面给予支持。鼓励和支持符合条件的数字经济企业通过股权投资、股票债券发行等方式融资，提高直接融资比例，改善融资结构。

第四十四条 数字基础设施依法受到保护。任何组织、个人不得侵占、损毁或者擅自迁移、拆除，不得实施非法侵入、干扰、破坏数字基础设施的活动，不得危害数字基础设施安全。

确因公共利益或者其他法定事由需要迁移、拆除数字基础设施的，应当依法给予补偿。

第四十五条 县级以上人民政府及其市场监督管理、知识产权、公安等主管部门应当加强数字经济领域知识产权保护，培育知识产权交易市场，探索建立知识产权保护规则和快速维权体系，依法打击知识产权侵权行为。

第四十六条 县级以上人民政府标准化行政主管部门应当会同有关部门组织依法制定数字经济相关地方标准，完善数字经济标准体系，对数字经济标准的实施进行监督。

支持行业协会、产业联盟等参与制定、修订数字经济国际规则、国际标准、国家标准、行业标准、地方标准。鼓励社会团体、企业制定满足市场和创新需要或者高于推荐性标准相关技术要求的团体标准、企业标准。

第四十七条 县级以上人民政府及其人力资源和社会保障等主管部门应当加强数字经济领域劳动用工服务指导，完善并落实平台经济、共享经济等新业态从业人员劳动保障权益方面政策规定。鼓励平台企业为从业人员购买商业保险，并依法开展新就业形态就业人员职业伤害保障工作。

第四十八条 县级以上人民政府及其有关部门应当按照优化传统服务与创新数字服务并行的原则，制定和完善老年人、残疾人等运用智能技术困难群体在出行、就医、消费、办事等方面的服务保障措施，提供适用的产品和服务，满足基本服务需求。

第四十九条 省人民政府及其数据、政务主管部门应当优化一网通办政务服务，推动一网统管省域治理，强化一网协同政府运行，以数字政府建设增强服务数字经济发展效能。

县级以上人民政府及其有关部门应当统筹推进社会治理数字化转型，建设运营综合治理工作平台、市场监管平台、综合执法平台、便民服务平台等基层治理平台，提高社会治理社会化、法治化、智能化和专业化水平，为数字经济发展营造良好环境。

第五十条 县级以上人民政府及其有关部门应当对数字经济领域新技术新产业新业态新模式等分类制定和实行监管规则及措施，根据实际制定发布包容免罚清单，留足发展空间，同时确保质量和安全，不得简单化予以禁止或者不予监管。

第五十一条 省、设区的市、自治州人民政府定期组织对本地区数字经济发展情况进行评估，并对下一级人民政府数字经济发展情况开展监督检查；必要时，可以委托第三方对数字经济发展情况进行评估。

第五十二条 国家机关工作人员在数字经济发展促进工作中存在滥用职权、玩忽职守、徇私舞弊等违法行为的，依法给予处分；构成犯罪的，依法追究刑事责任。

任何组织和个人违反网络安全、数据安全、个人信息保护等法律、法规的，由有关主管部门依法予以处罚；构成犯罪的，依法追究刑事责任。

第八章 附则

第五十三条 本办法自 2023 年 7 月 1 日起施行。

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

■ 工信部联网安〔2023〕95号

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，各银保监局，各相关单位：

网络安全保险是为网络安全风险提供保险保障的新兴险种，日益成为转移、防范网络安全风险的重要工具，在推进网络安全社会化服务体系建设中发挥着重要作用。为深入贯彻《中华人民共和国网络安全法》《中华人民共和国数据安全法》等相关法律法规，加快推动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，现提出如下意见。

一、建立健全网络安全保险政策标准体系

（一）完善网络安全保险政策制度。加强网络安全产业政策对网络安全保险的支持，推动网络安全技术服务赋能网络安全保险发展，引导关键信息基础设施保护、新兴融合领域网络安全保障等充分运用网络安全保险。加强保险业政策对网络安全保险的支持，指导网络安全保险创新发展，引导开发符合网络安全特点规律的保险产品。推动健全完善财政政策，充分利用地方首台（套）、首版（次）等现有政策，提供保险减税、保险购买补贴等措施。

（二）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，统一行业术语规范，明确核保、承保、理赔等主要环节基本流程和通用要求。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；承保中网络安全监测管理服务相关标准，规范监测预警方法；承保后理赔服务实施要求相关标准，规范网络安全保险售后服务。

二、加强网络安全保险产品服务创新

（三）丰富网络安全保险产品。鼓励保险公司面向不同行业场景的差异化网络安全风险管理需求，开发多元化网络安全保险产品。面向重点行业企业开发网络安全财产损失险、责任险和综合险等，提升企业网络安全风险应对能力。面向信息技术产品开发产品责任险，面向网络安全产品开发网络安全专门保险，为信息网络技术产品提供保险保障。面向网络安全服务开发职业责任险等产品，转移专业技术人员在安全服务过程中因人为操作可能引发的安全风险。

（四）创新发展网络安全保险服务。鼓励网络安全保险服务机构协同合作，探索构建以网络安全保险为核心的全流程网络安全风险管理解决方案。充分发挥保险机构专业优势，联合网络安全企业、基础电信运营商等加快网络安全保险与网络安全服务融合创新。充分发挥网络安全企业、专业网络安全测评机构技术优势，联合保险公司提升网络安全保险服务能力。

三、强化网络安全技术赋能保险发展

（五）开展网络安全风险量化评估。围绕电信和互联网行业典型事件以及工业互联网、车联网、物联网等新兴场景开展网络安全风险研究。探索建立网络安

全风险量化评估模型，加强网络安全风险影响规模预测、经济损失等分析。支持网络安全企业、专业网络安全测评机构等研发网络安全风险量化评估技术，开发轻量化网络安全风险量化评估工具，鼓励保险机构建立网络安全风险理赔数据库，支撑网络安全风险精准定价。

（六）加强网络安全风险监测能力。开展网络安全保险全生命周期风险监测，覆盖事前、事中、事后等重要环节。鼓励网络安全企业、专业网络安全测评机构等充分发挥网络安全风险监测技术优势，充分利用安全技术手段，针对网络安全漏洞、恶意网络资源、网络安全事件等开展网络安全威胁实时监测，及时发现网络安全风险隐患，提升网络安全风险监测预警、应急处置等能力。

四、促进网络安全产业需求释放

（七）推广网络安全保险服务应用。面向电信和互联网、能源、金融、医疗卫生等重点行业，以及工业互联网、车联网、物联网等新兴融合领域，围绕网络安全与信息技术产品服务供给侧和需求侧两类主体，充分发挥网络安全产业、网络安全保险相关联盟协会等作用，开展网络安全保险服务试点，形成可复制、可推广的网络安全保险服务模式，促进网络安全保险推广应用。

（八）推动企业网络安全风险应对能力提升。鼓励重点行业企业完善网络安全风险管理机制，推动电信和互联网、制造业、能源、金融、交通、水利、教育等重点行业企业积极利用网络安全保险工具，有效转移、防范网络安全风险，提升网络基础设施、重要信息系统和数据的安全防护能力。支持中小企业通过网络安全保险服务监控风险敞口，建立健全网络安全风险管理体系，不断加强中小企业网络安全防护能力。

五、培育网络安全保险发展生态

（九）培育优质网络安全保险企业。鼓励网络安全企业、保险机构积极参与网络安全保险生态建设，开展网络安全保险优秀案例征集、网络安全保险应用示范等活动，培育一批专业能力突出的保险机构，发展一批技术支撑能力领先的网络安全企业、专业网络安全测评机构等，建设一批网络安全保险创新联合体，培育网络安全保险发展良性生态。

（十）宣传推广网络安全保险服务。充分发挥相关行业联盟协会、重点企业带动作用，整合资源优势，促进网络安全产业和金融服务要素流动，开展网络安全保险教育培训，引导加强从业人员自律，规范网络安全保险推广应用。用好网络和数据安全产业高峰论坛、网络安全技术应用试点示范等活动，宣传普及网络安全保险，举办网络安全保险主题活动，加强经验总结和交流推广，营造促进网络安全保险规范健康发展的浓厚氛围。

工业和信息化部

国家金融监督管理总局

2023年7月2日

依法惩治网暴公开征求意见

为依法惩治网络暴力违法犯罪活动，最高法、最高检、公安部起草了《关于依法惩治网络暴力违法犯罪的指导意见（征求意见稿）》，现向社会公开征求意见。

意见指出，依法严惩网络暴力违法犯罪，对网络诽谤、网络侮辱、侵犯公民个人信息等行为准确适用法律。

①在信息网络上制造、散布谣言，贬损他人人格、损害他人名誉，情节严重，符合刑法第二百四十六条规定的，以诽谤罪定罪处罚。

②在信息网络上采取肆意谩骂、恶毒攻击、披露隐私等方式，公然侮辱他人，情节严重，符合刑法第二百四十六条规定的，以侮辱罪定罪处罚。

③组织“人肉搜索”，在信息网络上违法收集并向不特定多数人发布公民个人信息，情节严重，符合刑法第二百五十三条之一规定的，以侵犯公民个人信息罪定罪处罚。

④将网络暴力延伸至线下，对被网暴者及其亲友实施拦截辱骂、滋事恐吓、毁坏财物等滋扰行为，符合刑法第二百七十五条、第二百九十三条规定的，以故意毁坏财物罪、寻衅滋事罪定罪处罚。

⑤依法惩治借网络暴力事件实施的恶意营销炒作行为。网络服务提供者基于蹭炒热度、推广引流等目的，对于所发现的网络暴力信息不依法履行信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使违法信息大量传播或者有其他严重情节，符合刑法第二百八十六条之一规定的，以拒不履行信息网络安全管理义务罪定罪处罚；同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

指导意见指出，实施网络暴力违法犯罪，具有下列情形之一的，应当从重处罚：

①针对未成年人、残疾人实施的；

②组织“水军”“打手”实施的；

③编造“涉性”话题侵害他人人格尊严的；

④利用“深度合成”技术发布违法或者不良信息，违背公序良俗、伦理道德的；

⑤网络服务提供者发起、组织的。

央视网 2023-06-09 发表于北京

国家互联网信息办公室关于《规范和促进数据跨境流动规定（征求意见稿）》公开征求意见的通知

为保障国家数据安全，保护个人信息权益，进一步规范和促进数据依法有序自由流动，依据有关法律，我办起草了《规范和促进数据跨境流动规定（征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式提出反馈意见：

1. 登录中华人民共和国司法部 中国政府法制信息网（www.moj.gov.cn、www.chinalaw.gov.cn），进入首页主菜单的“立法意见征集”栏目提出意见。

2. 通过电子邮件将意见发送至：shujuju@cac.gov.cn。

3. 通过信函将意见寄至：北京市海淀区阜成路 15 号国家互联网信息办公室网络数据管理局，邮编：100048，并在信封上注明“规范和促进数据跨境流动规定征求意见”。

意见反馈截止时间为 2023 年 10 月 15 日。

附件：规范和促进数据跨境流动规定（征求意见稿）

国家互联网信息办公室

2023 年 9 月 28 日

规范和促进数据跨境流动规定（征求意见稿）

为保障国家数据安全，保护个人信息权益，进一步规范和促进数据依法有序自由流动，依据有关法律，对《数据出境安全评估办法》、《个人信息出境标准合同办法》等数据出境规定的施行，作出以下规定。

一、国际贸易、学术合作、跨国生产制造和市场营销等活动中产生的数据出境，不包含个人信息或者重要数据的，不需要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。

二、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。

三、不是在境内收集产生的个人信息向境外提供，不需要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。

四、符合以下情形之一的，不需要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所

必需，如跨境购物、跨境汇款、机票酒店预订、签证办理等，必须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人力资源管理，必须向境外提供内部员工个人信息的；

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

五、预计一年内向境外提供不满 1 万人个人信息的，不需要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。但是，基于个人同意向境外提供个人信息的，应当取得个人信息主体同意。

六、预计一年内向境外提供 1 万人以上、不满 100 万人个人信息，与境外接收方订立个人信息出境标准合同并向省级网信部门备案或者通过个人信息保护认证的，可以不申报数据出境安全评估；向境外提供 100 万人以上个人信息的，应当申报数据出境安全评估。但是，基于个人同意向境外提供个人信息的，应当取得个人信息主体同意。

七、自由贸易试验区可自行制定本自贸区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），报经省级网络安全和信息化委员会批准后，报国家网信部门备案。负面清单外数据出境，可以不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。

八、国家机关和关键信息基础设施运营者向境外提供个人信息和重要数据的，依照有关法律、行政法规、部门规章规定执行。向境外提供涉及党政军和涉密单位敏感信息、敏感个人信息的，依照有关法律、行政法规、部门规章规定执行。

九、数据处理者向境外提供重要数据和个人信息，应当遵守法律、行政法规的规定，履行数据安全保护义务，保障数据出境安全；发生数据出境安全事件或者发现数据出境安全风险增大的，应当采取补救措施，及时向网信部门报告。

十、各地方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，强化事前事中事后监管，发现数据出境活动存在较大风险或者发生安全事件的，要求数据处理者进行整改消除隐患；对拒不改正或者导致严重后果的，依法责令其停止数据出境活动，保障数据安全。

十一、《数据出境安全评估办法》、《个人信息出境标准合同办法》等相关规定与本规定不一致的，按照本规定执行。

来源：网信中国

国家互联网信息办公室关于《移动互联网未成年人模式建设指南（征求意见稿）》公开征求意见的通知

为切实强化未成年人网络保护，近年来，国家网信办指导网站平台持续推进青少年模式建设，扩大覆盖范围，优化功能设置，丰富适龄内容。模式自上线以来，普及率稳步提升，在帮助未成年人减少网络沉迷和不良信息影响方面发挥了积极作用。

为进一步提升模式效能，立足未成年人网络保护新形势新要求，国家网信办研究起草了《移动互联网未成年人模式建设指南（征求意见稿）》，将全面升级“青少年模式”为“未成年人模式”，推动模式覆盖范围由APP扩大到移动智能终端、应用商店，实现软硬件三方联动，方便用户一键进入模式，为未成年人营造安全健康的网络环境。现面向社会公开征求意见建议，欢迎社会各界积极参与。公众可通过以下途径和方式提出反馈意见：

1. 通过电子邮件方式发送至：wcnrms@cac.gov.cn。

2. 通过信函方式将意见寄至：北京市西城区车公庄大街11号国家互联网信息办公室网络综合治理局，邮编：100044，并请在信封上注明“移动互联网未成年人模式建设指南征求意见”字样。

意见反馈截止日期为2023年9月2日。

国家互联网信息办公室

2023年8月2日

移动互联网未成年人模式建设指南（征求意见稿）

一、目的依据

为了更好发挥互联网积极作用，营造良好网络环境，预防和干预未成年人网络沉迷问题，引导未成年人形成良好的网络使用习惯，按照《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《中华人民共和国未成年人保护法》等法律、行政法规，以及未成年人网络保护有关规定，制定本指南。

二、适用范围

本指南规定了各类移动智能终端、移动互联网应

用程序（以下简称“应用程序”）、移动互联网应用程序分发服务平台（以下简称“应用程序分发平台”）的未成年人模式应满足的基本要求、功能要求和管理要求，适用于移动智能终端提供者、应用程序提供者以及应用程序分发平台提供者等相关主体开展未成年人模式的研发和应用。

三、通用规范

（一）三方联动

移动智能终端、应用程序和应用程序分发平台之间应实现联动：

1、未成年人模式应具备自动切换功能。在移动智能终端一键启动未成年人模式后，应用程序、应用程序分发平台应自动切换到未成年人模式界面；在移动智能终端退出未成年人模式后，应用程序、应用程序分发平台应自动切换到普通模式界面。

2、未成年人模式应支持家长或未成年人用户通过账号在多移动智能终端（包括同一厂家的相同类型或不同类型的多个移动智能终端）进行统一设置。用户通过登录统一账号，自动将该账号下其他移动智能终端的已有配置复制到本地并开启。

3、移动智能终端、应用程序、应用程序分发平台之间应提供必要接口和数据共享，满足未成年人防沉迷提醒、家长监督管理等功能。

（二）便捷使用

1、为保护未成年人个人信息权益，鼓励家长为未成年人启动未成年人模式，移动智能终端、应用程序、应用程序分发平台应为家长管理提供便捷功能和服务，便于家长履行监护职责，引导未成年人形成良好上网习惯。

2、移动智能终端、应用程序、应用程序分发平台应当坚持最有利于未成年人的原则，提供有效识别违法信息和可能影响未成年人身心健康的信息、预防未成年人沉迷网络等功能，加强对未成年人的网络保护。

3、移动智能终端、应用程序、应用程序分发平台应在未成年人模式下建立便捷、合理、有效的投诉、举报渠道，及时受理处置涉未成年人投诉举报。

（三）分龄原则

移动智能终端、应用程序以及应用程序分发平台应根据不同年龄阶段的未成年人身心发展特点，通过评估产品的类型、内容与功能等要素，为不同年龄阶段用户提供适合其身心发展的信息和服务。分龄化设计根据以下 5 个年龄区间划分：

1. 不满 3 周岁；

2.3 周岁以上不满 8 周岁；

3.8 周岁以上不满 12 周岁；

4.12 周岁以上不满 16 周岁；

5.16 周岁以上不满 18 周岁。

四、移动智能终端未成年人模式要求

（一）基本要求

1. 未成年人模式入口

未成年人模式的入口设置应确保最简化原则。用户可通过开机提醒、桌面图标、系统设置等至少 3 种方式进入未成年人模式。模式入口应在固定位置、便捷易寻，满足家长和未成年人用户一键进入或切换。

用户在首次登录未成年人模式时，移动智能终端应在入口提供设置生日、选择年龄或年龄区间等多种方式供用户自行选择，并允许设置多个未成年人信息。

用户可在首次开机或系统设置选择不需要未成年人模式，系统将不再出现相关提醒。

2. 未成年人模式退出

从未成年人模式退出时，需要家长进行验证同意，家长可基于现有移动智能终端认证机制，自行选择密码、指纹、人脸等识别方式进行单一或复合验证。

（二）使用时长管理

1. 移动智能终端应为不同年龄段的未成年人用户提供差异化使用时长管理服务。当超过每日使用时限，移动智能终端应自动关闭除特定必要应用程序和家长自定义豁免的应用程序之外的其他应用程序：

（1）在面向不满 8 周岁用户的未成年人模式中，移动智能终端应支持默认使用总时长不超过 40 分钟，

同时提供家长豁免操作；

（2）在面向 8 周岁以上不满 16 周岁用户的未成年人模式中，移动智能终端应支持默认使用总时长不超过 1 小时，同时提供家长豁免操作；

（3）在面向 16 周岁以上不满 18 周岁用户的未成年人模式中，移动智能终端应支持默认使用总时长不超过 2 小时，同时提供家长豁免操作；

（4）在未成年人模式下，当未成年人用户连续使用移动智能终端时长超过 30 分钟，移动智能终端应发出休息提醒；

（5）在未成年人模式下，移动智能终端每日 22 时至次日 6 时期间禁止向未成年人提供服务；

（6）以下应用程序和业务不受上述使用时长和时间段限制：

①应急类：用于保障未成年人人身安全的产品和服务，包括紧急呼叫业务及移动智能终端自定义的用于保障未成年人的人身安全的应用程序；

②教育类：在有关主管部门备案的，为未成年人提供网课等教育服务的产品和服务；

③适合未成年人使用的工具类：经应用程序分发平台认证的，适合未成年人身心发展的产品和服务，如部分图像处理、计算测量应用程序等；

④家长自定义设置可被豁免的应用程序。

2. 在移动智能终端的未成年人模式中，家长使用时间管控功能应至少满足如下功能：

（1）设置移动智能终端整机使用时长；

（2）设置移动智能终端整机使用时间段，可根据具体需要，设置某个或者多个使用时间段；

（3）设置指定应用程序使用时间；

（4）禁止未成年人修改移动智能终端的系统日期和时间。

（三）防绕过要求

1. 移动智能终端应具备防绕过功能。在进入未成年人模式后，移动智能终端应在家长验证并确认后才能执行退出未成年人模式或恢复出厂设置等操作。

2. 开启未成年人模式的移动智能终端应确保提供未成年人模式服务功能的图标始终保持在桌面一级页面，不被卸载、冻结和隐藏，进程不被强制结束。

3. 在未成年人模式下，如需启动开发者模式，应经家长验证并确认。

（四）补充要求

1. 由于未成年人的视觉、听觉等生理和心理尚未发育成熟，鼓励移动智能终端利用技术手段降低或消除未成年人在使用移动智能终端过程中可能出现的危害。

2. 移动智能终端应提供未成年人用户紧急向关联的家长用户终端发送位置和进行呼叫的服务。

3. 儿童智能手表、早教机、智能音箱等儿童智能设备，及虚拟现实 / 增强现实（VR/AR）可穿戴设备在为未成年人提供服务时，应遵守本规定中的相关条款，确保信息内容安全可控，防范未成年人产生网络沉迷或接触可能影响身心健康的信息。

4. 现有应用程序中的青少年模式，应在移动智能终端普通模式下予以保留，并按照本指南的有关要求进行升级改造，为未成年人在普通模式下使用现有应用程序提供安全防护。

五、移动互联网应用程序未成年人模式要求

（一）基本要求

在未成年人模式下移动互联网信息服务提供者应为未成年人提供分龄内容服务，并打造专属内容池。适龄推荐内容如下：

1. 不满 3 周岁：推荐儿歌、启蒙教育等亲子陪伴类节目内容，建议以音频为主；

2.3 周岁以上不满 8 周岁: 推荐启蒙教育、兴趣素养、通识教育等节目内容；

3.8 周岁以上不满 12 周岁：推荐通识教育、知识科普、生活技能、具有正向引导意义的娱乐性内容和适合本年龄段认知能力的新闻资讯等；

4.12 周岁以上不满 16 周岁：推荐通识教育、学科教育、知识科普、生活技能、具有正向引导意义的娱乐性内容和适合本年龄段认知能力的新闻资讯等。

5.16 周岁以上不满 18 周岁：推荐适合本年龄段认

知能力、健康向上的信息内容。

鼓励移动互联网信息服务提供者根据分龄要求对未成年人专属内容池中的内容进行适龄推荐标注。

（二）内容安全要求

在未成年人模式下移动互联网信息服务提供者应履行主体责任，保障未成年人接触的信息内容安全：

1. 在未成年人模式下移动互联网信息服务提供者应积极开展未成年人内容池建设。制作、复制、发布、传播弘扬社会主义核心价值观和社会主义先进文化、革命文化、中华优秀传统文化，铸牢中华民族共同体意识，培养未成年人家国情怀和良好品德，引导未成年人养成良好生活习惯和行为习惯等的网络信息，营造有利于未成年人健康成长的清朗网络空间和良好网络生态。

2. 移动互联网信息服务提供者应履行主体责任，在未成年人模式下不应出现任何形式向未成年人用户提供诱导其沉迷或不利于其身心健康的相关产品和服务：

（1）禁止利用网络制作、复制、发布、传播含有危害未成年人身心健康内容的信息，禁止向未成年人发送含有危害或者可能影响未成年人身心健康内容的信息；

（2）禁止制作、复制、发布、传播或者持有有关未成年人的淫秽色情网络信息，禁止诱骗、强迫未成年人制作、复制、发布、传播可能暴露其个人隐私的文字、图片、音视频；

（3）禁止制作、复制、发布、传播可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生不良情绪、养成不良嗜好等可能影响未成年人身心健康的信息。

（三）功能限制要求

在未成年人模式下移动互联网信息服务提供者应限制未成年人用户使用可能危害其身心健康的产品和服务：

1. 网络直播、网络音视频、网络社交等网络服务提供者应针对未成年人使用其服务设置相应的时间管理、权限管理、消费管理等功能。

2. 网络直播、网络音视频、网络社交等网络服务提供者应采取措施，合理限制未成年人在使用网络产品和服务中的单次消费数额和单日累计消费数额，不得向未成年人提供与其民事行为能力不符的付费服务。

3. 未成年人模式下不得设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，不得利用泛娱乐化功能和内容诱导未成年人沉迷网络。

4. 网络游戏的防沉迷要求应遵守相关管理规定。

5. 在线教育网络产品和服务不得插入网络游戏链

接，不得推送广告等与教学无关的信息。

6. 算法推荐服务提供者不得向未成年人推送可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等可能影响未成年人身心健康的信息，不得利用算法推荐服务诱导未成年人沉迷网络。

7. 鼓励应用程序开发者遵照相关法律法规，开发适应未成年人身心健康发展规律和特点的应用程序，帮助未成年人培养良好网络素养。

（四）社交管理要求

1. 应用程序应为未成年人及家长提供社交管理权限，允许关注或屏蔽特定用户，限定特定信息的公开范围。

2. 社交类应用程序不应在未成年人模式中为容易产生网络沉迷或使未成年人接触不利于其身心健康的互联网信息提供外链。

3. 除即时通讯工具以外的应用程序，在未成年人模式下应关闭陌生人私信功能。

六、移动互联网应用程序分发服务平台未成年人模式要求

（一）基本要求

1. 应用程序分发平台应提供未成年人应用专区，便利未成年人获取有益身心健康的平台内产品或者服务；

2. 应用程序分发平台应根据不同年龄段未成年人的身心特点和认知水平，标注应用程序的推荐年龄，提供适宜不同年龄段未成年人的应用程序。

（二）未成年人专区建设要求

应用程序分发平台应根据相关管理要求，加强未成年人专区建设：

1. 应用程序提供者应当坚持最有利于未成年人的原则，关注未成年人健康成长，履行未成年人网络保护各项义务，严格落实未成年人用户账号实名注册和登录要求，不得以任何形式向未成年人用户提供诱导其沉迷的相关产品和服务。

2. 鼓励教育、益智、科普、读书、音乐、体育等有利于未成年人身心健康的应用程序在未成年人专区中上架。

3. 有关部门针对各年龄段特点明确禁用的应用程序，不得在未成年人模式下的应用程序分发平台上架。

（三）下载安全

应用程序分发平台应根据有关法律法规对各类网络应用程序和服务准入未成年人模式进行审核和处置：

1. 明确产品所适合的未成年人用户年龄阶段，并在用户下载、注册、登录界面等位置显著提示。

2. 应用程序分发平台应根据未成年人的年龄特点，为未成年人用户提供差异化下载服务，并确保家长可以对未成年人模式下的应用程序下载和安装进行审核或豁免：

（1）不满 12 周岁的未成年人用户下载、安装未成年人专区中的应用程序时，需经家长同意；家长具备一定的豁免权力，允许未成年人下载未成年人专区以外的应用程序；

（2）12 周岁以上不满 16 周岁的未成年人用户可自行下载、安装未成年人专区中的应用程序，家长具备一定的豁免权力，允许未成年人下载未成年人专区以外的应用程序。

3. 禁止通过外链下载应用程序，家长审核并豁免的除外。

4. 应用程序分发平台应建立相关举报机制，加强用户对未成年人模式中的信息内容与服务进行监督，必要时根据相关管理要求对有关应用程序予以下架处理。

七、家长管理

（一）基本要求

未成年人模式下，移动智能终端、应用程序、应用程序分发平台应为家长提供管理权限，保障家长能够对指定的未成年人用户进行日常和应急状态管理，更好监督引导未成年人用户上网行为：

1. 移动智能终端、应用程序、应用程序分发平台应为家长提供对未成年人使用时长、信息服务接收、应用程序下载安装等方面的管理权限，满足家长对未成

年人用户的监督、豁免和审核需求。

2. 移动智能终端应为未成年人账号提供至少 1 个亲情号绑定作为家长账号，该账号可满足家长与未成年人同终端和异终端使用，并可同时关联应用程序和应用程序分发平台。

（二）家长对未成年人移动智能终端使用时间的管理

移动智能终端和应用程序应为未成年人及其家长提供防沉迷提醒，允许家长对未成年人移动智能终端的使用时间进行监督指导：

1. 移动智能终端应定期向家长提供未成年人用户在未成年人模式下的使用时长、各应用程序使用时长、上网时长等概览报告，协助家长对未成年人网络行为进行监督。

2. 当未成年人用户的使用时长超过本规定所建议的时间限制时，可由未成年人用户向关联的家长用户发出豁免申请。

（三）家长对未成年人信息服务内容的管理

家长可以使用关联账号对未成年人模式下的信息内容提供审核和豁免功能：

1. 家长可对非专属内容池的信息进行豁免，加入到指定未成年人用户的内容池中。

2. 鼓励家长对非专属内容池的内容进行标注和建议，为平台丰富专属内容池建设提供依据。

（四）家长对未成年人应用程序使用的管理

家长可以使用关联账号对未成年人模式下的应用程序下载进行审核，豁免或禁止用户下载及安装特定应用程序。包括：

1. 为特定应用程序开放始终豁免的权限，如对辅助教育类应用程序开放未成年人长期使用权限。

2. 为特定应用程序开放限时使用权限，如根据需要，对适合未成年人身心发展的工具类应用程序开放特定时间段内使用的权限。

3. 将特定应用程序和功能设置为始终禁止使用，期间相关应用程序不得弹出通知，不得被调取使用。

4. 相关法规明令禁止未成年人使用的应用程序和服务，不得被豁免。

八、管理要求

（一）移动智能终端、应用程序、应用程序分发平台应积极配合有关管理部门开展的监督检查，提供必要的技术、数据等支持和协助。

（二）向未成年人用户提供服务的移动智能终端、应用程序、应用程序分发平台，应定期开展未成年人网络保护影响评估。

（三）向未成年人用户提供服务的移动智能终端、应用程序、应用程序分发平台，应建立必要应急响应机制，确保保护未成年人用户人身安全的应急类业务不被屏蔽。

（四）在未成年人模式下移动互联网信息服务提供者应依照相关法律法规提供服务，不应超范围收集用户数据。

附录 术语和定义

（1）未成年人模式

本《指南》所称未成年人模式，是指适应未成年人身心健康发展规律和特点，专门面向未成年人使用，覆盖移动智能终端、移动互联网应用程序和移动互联网应用程序分发平台的网络保护模式。

（2）移动智能终端

移动智能终端是指接入公众移动通信网络、具有操作系统、可由用户自行安装运行和卸载应用程序的移动终端产品，包括智能手机、平板电脑、儿童智能手表、早教机等智能终端和智能可穿戴设备。

（3）移动互联网应用程序

移动互联网应用程序指通过应用程序向用户提供文字、图片、音频、视频等信息制作、复制、发布、传播等服务的软件。

（4）移动互联网应用程序分发服务平台

移动互联网应用程序分发服务平台指通过互联网提供应用程序发布、下载、动态加载等服务的平台，包括应用商店、应用中心、互联网小程序平台等。

李强签署国务院令 公布《未成年人网络保护条例》

中华人民共和国国务院令

第766号

《未成年人网络保护条例》已经 2023 年 9 月 20 日国务院第 15 次常务会议通过，现予公布，自 2024 年 1 月 1 日起施行。

总理 李强

2023 年 10 月 16 日

未成年人网络保护条例

第一章 总则

第一条 为了营造有利于未成年人身心健康的网络环境，保障未成年人合法权益，根据《中华人民共和国未成年人保护法》、《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条 未成年人网络保护工作应当坚持中国共产党的领导，坚持以社会主义核心价值观为引领，坚持最有利于未成年人的原则，适应未成年人身心健康发展和网络空间的规律和特点，实行社会共治。

第三条 国家网信部门负责统筹协调未成年人网络保护工作，并依据职责做好未成年人网络保护工作。

国家新闻出版、电影部门和国务院教育、电信、公安、民政、文化和旅游、卫生健康、市场监督管理、广播电视等有关部门依据各自职责做好未成年人网络保护工作。

县级以上地方人民政府及其有关部门依据各自职责做好未成年人网络保护工作。

第四条 共产主义青年团、妇女联合会、工会、残疾人联合会、关心下一代工作委员会、青年联合会、学生联合会、少年先锋队以及其他人民团体、有关社会组织、基层群众性自治组织，协助有关部门做好未成年人网络保护工作，维护未成年人合法权益。

第五条 学校、家庭应当教育引导未成年人参加有益身心健康的活动，科学、文明、安全、合理使用网络，预防和干预未成年人沉迷网络。

第六条 网络产品和服务提供者、个人信息处理者、智能终端产品制造者和销售者应当遵守法律、行政法规和国家有关规定，尊重社会公德，遵守商业道德，诚实信用，履行未成年人网络保护义务，承担社会责任。

第七条 网络产品和服务提供者、个人信息处理者、

智能终端产品制造者和销售者应当接受政府和社会的监督，配合有关部门依法实施涉及未成年人网络保护工作的监督检查，建立便捷、合理、有效的投诉、举报渠道，通过显著方式公布投诉、举报途径和方法，及时受理并处理公众投诉、举报。

第八条 任何组织和个人发现违反本条例规定的，可以向网信、新闻出版、电影、教育、电信、公安、民政、文化和旅游、卫生健康、市场监督管理、广播电视等有关部门投诉、举报。收到投诉、举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

第九条 网络相关行业组织应当加强行业自律，制定未成年人网络保护相关行业规范，指导会员履行未成年人网络保护义务，加强对未成年人的网络保护。

第十条 新闻媒体应当通过新闻报道、专题栏目（节目）、公益广告等方式，开展未成年人网络保护法律法规、政策措施、典型案例和有关知识的宣传，对侵犯未成年人合法权益的行为进行舆论监督，引导全社会共同参与未成年人网络保护。

第十一条 国家鼓励和支持在未成年人网络保护领域加强科学研究和人才培养，开展国际交流与合作。

第十二条 对在未成年人网络保护工作中作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 网络素养促进

第十三条 国务院教育部门应当将网络素养教育纳入学校素质教育内容，并会同国家网信部门制定未成年人网络素养测评指标。

教育部门应当指导、支持学校开展未成年人网络素养教育，围绕网络道德意识形成、网络法治观念培养、网络使用能力建设、人身财产安全保护等，培育未成年人网络安全意识、文明素养、行为习惯和防护技能。

第十四条 县级以上人民政府应当科学规划、合理布局，促进公益性上网服务均衡协调发展，加强提供公益性上网服务的公共文化设施建设，改善未成年人上网条件。

县级以上地方人民政府应当通过为中小学校配备具有相应专业能力的指导教师、政府购买服务或者鼓励中小学校自行采购相关服务等方式，为学生提供优质的网络素养教育课程。

第十五条 学校、社区、图书馆、文化馆、青少年宫等场所为未成年人提供互联网上网服务设施的，应当通过安排专业人员、招募志愿者等方式，以及安装未成年人网络保护软件或者采取其他安全保护技术措施，为未成年人提供上网指导和安全、健康的上网环境。

第十六条 学校应当将提高学生网络素养等内容纳入教育教学活动，并合理使用网络开展教学活动，建立健全学生在校期间上网的管理制度，依法规范管理未成年学生带入学校的智能终端产品，帮助学生养成良好上网习惯，培养学生网络安全和网络法治意识，增强学生对网络信息的获取和分析判断能力。

第十七条 未成年人的监护人应当加强家庭家教家风建设，提高自身网络素养，规范自身使用网络的行为，加强对未成年人使用网络行为的教育、示范、引导和监督。

第十八条 国家鼓励和支持研发、生产和使用专门以未成年人为服务对象、适应未成年人身心健康发展规律和特点的网络保护软件、智能终端产品和未成年人模式、未成年人专区等网络技术、产品、服务，加强网络无障碍环境建设和改造，促进未成年人开阔眼界、陶冶情操、提高素质。

第十九条 未成年人网络保护软件、专门供未成年人使用的智能终端产品应当具有有效识别违法信息和可能影响未成年人身心健康的信息、保护未成年人个人信息权益、预防未成年人沉迷网络、便于监护人履行监护职责等功能。

国家网信部门会同国务院有关部门根据未成年人网络保护工作的需要，明确未成年人网络保护软件、专门供未成年人使用的智能终端产品的相关技术标准或者要求，指导监督网络相关行业组织按照有关技术标准和要求对未成年人网络保护软件、专门供未成年人

使用的智能终端产品的使用效果进行评估。

智能终端产品制造者应当在产品出厂前安装未成年人网络保护软件，或者采用显著方式告知用户安装渠道和方法。智能终端产品销售者在产品销售前应当采用显著方式告知用户安装未成年人网络保护软件的情况以及安装渠道和方法。

未成年人的监护人应当合理使用并指导未成年人使用网络保护软件、智能终端产品等，创造良好的网络使用家庭环境。

第二十条 未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者，应当履行下列义务：

（一）在网络平台服务的设计、研发、运营等阶段，充分考虑未成年人身心健康发展特点，定期开展未成年人网络保护影响评估；

（二）提供未成年人模式或者未成年人专区等，便利未成年人获取有益身心健康的平台内产品或者服务；

（三）按照国家规定建立健全未成年人网络保护合规制度体系，成立主要由外部成员组成的独立机构，对未成年人网络保护情况进行监督；

（四）遵循公开、公平、公正的原则，制定专门的平台规则，明确平台内产品或者服务提供者的未成年人网络保护义务，并以显著方式提示未成年人用户依法享有的网络保护权利和遭受网络侵害的救济途径；

（五）对违反法律、行政法规严重侵害未成年人身心健康或者侵犯未成年人其他合法权益的平台内产品或者服务提供者，停止提供服务；

（六）每年发布专门的未成年人网络保护社会责任报告，并接受社会监督。

前款所称的未成年人用户数量巨大或者对未成年人群体具有显著影响的网络平台服务提供者的具体认定办法，由国家网信部门会同有关部门另行制定。

第三章 网络信息内容规范

第二十一条 国家鼓励和支持制作、复制、发布、传播弘扬社会主义核心价值观和社会主义先进文化、革命文化、中华优秀传统文化，铸牢中华民族共同体意识，培养未成年人家国情怀和良好品德，引导未成年人养成良好生活习惯和行为习惯等的网络信息，营造有利于未成年人健康成长的清朗网络空间和良好网络生态。

第二十二条 任何组织和个人不得制作、复制、发布、传播含有宣扬淫秽、色情、暴力、邪教、迷信、赌博、引诱自残自杀、恐怖主义、分裂主义、极端主义等危害未成年人身心健康内容的网络信息。

任何组织和个人不得制作、复制、发布、传播或者持有有关未成年人的淫秽色情网络信息。

第二十三条 网络产品和服务中含有可能引发或者诱导未成年人模仿不安全行为、实施违反社会公德行为、产生极端情绪、养成不良嗜好等可能影响未成年人身心健康的信息的，制作、复制、发布、传播该信息的组织和个人应当在信息展示前予以显著提示。

国家网信部门会同国家新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、广播电视等部门，在前款规定基础上确定可能影响未成年人身心健康的信息的具体种类、范围、判断标准和提示办法。

第二十四条 任何组织和个人不得在专门以未成年人为服务对象的网络产品和服务中制作、复制、发布、传播本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。

网络产品和服务提供者不得在首页首屏、弹窗、热搜等处于产品或者服务醒目位置、易引起用户关注的重点环节呈现本条例第二十三条第一款规定的可能影响未成年人身心健康的信息。

网络产品和服务提供者不得通过自动化决策方式向未成年人进行商业营销。

第二十五条 任何组织和个人不得向未成年人发送、推送或者诱骗、强迫未成年人接触含有危害或者可能影响未成年人身心健康内容的网络信息。

第二十六条 任何组织和个人不得通过网络以文字、图片、音视频等形式，对未成年人实施侮辱、诽谤、威胁或者恶意损害形象等网络欺凌行为。

网络产品和服务提供者应当建立健全网络欺凌行

为的预警预防、识别监测和处置机制，设置便利未成年人及其监护人保存遭受网络欺凌记录、行使通知权利的功能、渠道，提供便利未成年人设置屏蔽陌生用户、本人发布信息可见范围、禁止转载或者评论本人发布信息、禁止向本人发送信息等网络欺凌信息防护选项。

网络产品和服务提供者应当建立健全网络欺凌信息特征库，优化相关算法模型，采用人工智能、大数据等技术手段和人工审核相结合的方式加强对网络欺凌信息的识别监测。

第二十七条 任何组织和个人不得通过网络以文字、图片、音视频等形式，组织、教唆、胁迫、引诱、欺骗、帮助未成年人实施违法犯罪行为。

第二十八条 以未成年人为服务对象的在线教育网络产品和服务提供者，应当按照法律、行政法规和国家有关规定，根据不同年龄阶段未成年人身心发展特点和认知能力提供相应的产品和服务。

第二十九条 网络产品和服务提供者应当加强对用户发布信息的管理，采取有效措施防止制作、复制、发布、传播违反本条例第二十二条、第二十四条、第二十五条、第二十六条第一款、第二十七条规定的信息，发现违反上述条款规定的信息的，应当立即停止传输相关信息，采取删除、屏蔽、断开链接等处置措施，防止信息扩散，保存有关记录，向网信、公安等部门报告，并对制作、复制、发布、传播上述信息的用户采取警示、限制功能、暂停服务、关闭账号等处置措施。

网络产品和服务提供者发现用户发布、传播本条例第二十三条第一款规定的信息未予显著提示的，应当作出提示或者通知用户予以提示；未作出提示的，不得传输该信息。

第三十条 国家网信、新闻出版、电影部门和国务院教育、电信、公安、文化和旅游、广播电视等部门发现违反本条例第二十二条、第二十四条、第二十五条、第二十六条第一款、第二十七条规定的信息的，或者发现本条例第二十三条第一款规定的信息未予显著提示的，应当要求网络产品和服务提供者按照本条例第二十九条的规定予以处理；对来源于境外的上述信息，应当依法通知有关机构采取技术措施和其他必要措施阻断传播。

第四章 个人信息网络保护

第三十一条 网络服务提供者为未成年人提供信息发布、即时通讯等服务的，应当依法要求未成年人或者其监护人提供未成年人真实身份信息。未成年人或者其监护人不提供未成年人真实身份信息的，网络服务提供者不得为未成年人提供相关服务。

网络直播服务提供者应当建立网络直播发布者真实身份信息动态核验机制，不得向不符合法律规定情形的未成年人用户提供网络直播发布服务。

第三十二条 个人信息处理者应当严格遵守国家网信部门和有关部门关于网络产品和服务必要个人信息范围的规定，不得强制要求未成年人或者其监护人同意非必要的个人信息处理行为，不得因为未成年人或者其监护人不同意处理未成年人非必要个人信息或者撤回同意，拒绝未成年人使用其基本功能服务。

第三十三条 未成年人的监护人应当教育引导未成年人增强个人信息保护意识和能力、掌握个人信息范围、了解个人信息安全风险，指导未成年人行使其在个人信息处理活动中的查阅、复制、更正、补充、删除等权利，保护未成年人个人信息权益。

第三十四条 未成年人或者其监护人依法请求查阅、复制、更正、补充、删除未成年人个人信息的，个人信息处理者应当遵守以下规定：

（一）提供便捷的支持未成年人或者其监护人查阅未成年人个人信息种类、数量等的方法和途径，不得对未成年人或者其监护人的合理请求进行限制；

（二）提供便捷的支持未成年人或者其监护人复制、更正、补充、删除未成年人个人信息的功能，不得设置不合理条件；

（三）及时受理并处理未成年人或者其监护人查阅、复制、更正、补充、删除未成年人个人信息的申请，拒绝未成年人或者其监护人行使权利的请求的，应当书面告知申请人并说明理由。

对未成年人或者其监护人依法提出的转移未成年人个人信息的请求，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径。

第三十五条 发生或者可能发生未成年人个人信息泄露、篡改、丢失的，个人信息处理者应当立即启动个人信息安全事件应急预案，采取补救措施，及时向网信等部门报告，并按照国家有关规定将事件情况以邮件、信函、电话、信息推送等方式告知受影响的未成年人及其监护人。

个人信息处理者难以逐一告知的，应当采取合理、有效的方式及时发布相关警示信息，法律、行政法规另有规定的除外。

第三十六条 个人信息处理者对其工作人员应当以最小授权为原则，严格设定信息访问权限，控制未成年人个人信息知悉范围。工作人员访问未成年人个人信息的，应当经过相关负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法处理未成年人个人信息。

第三十七条 个人信息处理者应当自行或者委托专业机构每年对其处理未成年人个人信息遵守法律、行政法规的情况进行合规审计，并将审计情况及时报告网信等部门。

第三十八条 网络服务提供者发现未成年人私密信息或者未成年人通过网络发布的个人信息中涉及私密信息的，应当及时提示，并采取停止传输等必要保护措施，防止信息扩散。

网络服务提供者通过未成年人私密信息发现未成年人可能遭受侵害的，应当立即采取必要措施保存有关记录，并向公安机关报告。

第五章 网络沉迷防治

第三十九条 对未成年人沉迷网络进行预防和干预，应当遵守法律、行政法规和国家有关规定。

教育、卫生健康、市场监督管理等部门依据各自职责对从事未成年人沉迷网络预防和干预活动的机构实施监督管理。

第四十条 学校应当加强对教师的指导和培训，提高教师对未成年学生沉迷网络的早期识别和干预能力。对于有沉迷网络倾向的未成年学生，学校应当及时告知其监护人，共同对未成年学生进行教育和引导，帮助其恢复正常的学习生活。

第四十一条 未成年人的监护人应当指导未成年人安全合理使用网络，关注未成年人上网情况以及相关生理状况、心理状况、行为习惯，防范未成年人接触危害或者可能影响其身心健康的网络信息，合理安排未成年人使用网络的时间，预防和干预未成年人沉迷网络。

第四十二条 网络产品和服务提供者应当建立健全防沉迷制度，不得向未成年人提供诱导其沉迷的产品和服务，及时修改可能造成未成年人沉迷的内容、功能和规则，并每年向社会公布防沉迷工作情况，接受社会监督。

第四十三条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当针对不同年龄阶段未成年人使用其服务的特点，坚持融合、友好、实用、有效的原则，设置未成年人模式，在使用时段、时长、功能和内容等方面按照国家有关规定和标准提供相应的服务，并以醒目便捷的方式为监护人履行监护职责提供时间管理、权限管理、消费管理等功能。

第四十四条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当采取措施，合理限制不同年龄阶段未成年人在使用其服务中的单次消费数额和单日累计消费数额，不得向未成年人提供与其民事行为能力不符的付费服务。

第四十五条 网络游戏、网络直播、网络音视频、网络社交等网络服务提供者应当采取措施，防范和抵制流量至上等不良价值倾向，不得设置以应援集资、投票打榜、刷量控评等为主题的网络社区、群组、话题，不得诱导未成年人参与应援集资、投票打榜、刷量控评等网络活动，并预防和制止其用户诱导未成年人实施上述行为。

第四十六条 网络游戏服务提供者应当通过统一的未成年人网络游戏电子身份认证系统等必要手段验证未成年人用户真实身份信息。

网络产品和服务提供者不得为未成年人提供游戏账号租售服务。

第四十七条 网络游戏服务提供者应当建立、完善预防未成年人沉迷网络的游戏规则，避免未成年人接触可能影响其身心健康的游戏内容或者游戏功能。

网络游戏服务提供者应当落实适龄提示要求，根据不同年龄阶段未成年人身心发展特点和认知能力，通过评估游戏产品的类型、内容与功能等要素，对游戏产品进行分类，明确游戏产品适合的未成年人用户年龄阶段，并在用户下载、注册、登录界面等位置予以显著提示。

第四十八条 新闻出版、教育、卫生健康、文化和旅游、广播电视、网信等部门应当定期开展预防未成年人沉迷网络的宣传教育，监督检查网络产品和服务提供者履行预防未成年人沉迷网络义务的情况，指导家庭、学校、社会组织互相配合，采取科学、合理的方式对未成年人沉迷网络进行预防和干预。

国家新闻出版部门牵头组织开展未成年人沉迷网络游戏防治工作，会同有关部门制定关于向未成年人提供网络游戏服务的时段、时长、消费上限等管理规定。

卫生健康、教育等部门依据各自职责指导有关医疗卫生机构、高等学校等，开展未成年人沉迷网络所致精神障碍和心理行为问题的基础研究和筛查评估、诊断、预防、干预等应用研究。

第四十九条 严禁任何组织和个人以虐待、胁迫等侵害未成年人身心健康的方式干预未成年人沉迷网络、侵犯未成年人合法权益。

第六章 法律责任

第五十条 地方各级人民政府和县级以上有关部门违反本条例规定，不履行未成年人网络保护职责的，由其上级机关责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。

第五十一条 学校、社区、图书馆、文化馆、青少

年宫等违反本条例规定，不履行未成年人网络保护职责的，由教育、文化和旅游等部门依据各自职责责令改正；拒不改正或者情节严重的，对负有责任的领导人员和直接责任人员依法给予处分。

第五十二条 未成年人的监护人不履行本条例规定的监护职责或者侵犯未成年人合法权益的，由未成年人居住地的居民委员会、村民委员会、妇女联合会，监护人所在单位，中小学校、幼儿园等有关密切接触未成年人的单位依法予以批评教育、劝诫制止、督促其接受家庭教育指导等。

第五十三条 违反本条例第七条、第十九条第三款、第三十八条第二款规定的，由网信、新闻出版、电影、教育、电信、公安、民政、文化和旅游、市场监督管理、广播电视等部门依据各自职责责令改正；拒不改正或者情节严重的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第五十四条 违反本条例第二十条第一款规定的，由网信、新闻出版、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正，给予警告，没收违法所得；拒不改正的，并处 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

违反本条例第二十条第一款第一项和第五项规定，情节严重的，由省级以上网信、新闻出版、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正，没收违法所得，并处 5000 万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关部门依法吊销相关业务许可证或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处 10 万元以上 100 万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和未成年人保护负责人。

第五十五条 违反本条例第二十四条、第二十五条规定的，由网信、新闻出版、电影、电信、公安、文化和旅游、市场监督管理、广播电视等部门依据各自职责责令限期改正，给予警告，没收违法所得，可以并处 10 万元以下罚款；拒不改正或者情节严重的，责令暂停相关业务、停产停业或者吊销相关业务许可证、吊销营业执照，违法所得 100 万元以上的，并处违法所得 1 倍以上 10 倍以下罚款，没有违法所得或者违法所得不足 100 万元的，并处 10 万元以上 100 万元以下罚款。

第五十六条 违反本条例第二十六条第二款和第三款、第二十八条、第二十九条第一款、第三十一条第二款、第三十六条、第三十八条第一款、第四十二条至第四十五条、第四十六条第二款、第四十七条规定的，由网信、新闻出版、电影、教育、电信、公安、文化和旅游、广播电视等部门依据各自职责责令改正，给予警告，没收违法所得，违法所得 100 万元以上的，并处违法所得 1 倍以上 10 倍以下罚款，没有违法所得或者违法所得不足 100 万元的，并处 10 万元以上 100 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；拒不改正或者情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

第五十七条 网络产品和服务提供者违反本条例规定，受到关闭网站、吊销相关业务许可证或者吊销营业执照处罚的，5 年内不得重新申请相关许可，其直接负责的主管人员和其他直接责任人员 5 年内不得从事同类网络产品和服务业务。

第五十八条 违反本条例规定，侵犯未成年人合法权益，给未成年人造成损害的，依法承担民事责任；构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七章 附则

第五十九条 本条例所称智能终端产品，是指可以接入网络、具有操作系统、能够由用户自行安装应用软件的手机、计算机等网络终端产品。

第六十条 本条例自 2024 年 1 月 1 日起施行。

武网安协与汇科智创党支部联合主题党日活动顺利开展

为进一步提升主题党日活动质量，丰富主题党日活动内涵，强化党员干部的凝聚力和战斗力，更好发挥党员的先锋模范作用，促使党建与业务工作高度融合，近日，中共武汉市网络安全协会支部与中共武汉汇科智创科技有限公司支部联合举办主题党日活动。双方支部全体党员参加，本次活动我会党支部还特别邀请了中国联通武汉分公司、神州绿盟武汉分公司、武汉德发等会员单位的党员代表共同参与学习交流。会议由汇科智创公司常务副总经理向仕华主持。

会前，全体党员参观了汉阳市政企业展厅，了解汉阳市政集团 70 周年风雨历程，充分展示汉阳市政集团一路走来的实力与担当。

随后，双方参观了汇科智创数字化展厅，就正在建设中的汉阳区 CIM 平台展开交流与讨论。

随后开始学习交流环节。向仕华对武汉市网络安全协会一行的到来表示欢迎，并对汇科智创公司业务进行简要介绍，他表示，汇科智创公司致力于打造一支“数智化引领的党支部”，坚持党的领导核心，积极在把方向、管大局、促落实等方面发挥党的领导作用。

随后全体党员重温了入党誓词，学习了近期习近平总书记重要讲话内容。武汉市网络安全协会轮值会

长、武汉安域信息安全技术有限公司总经理周佑源带来了专题演讲。他对网络安全法规体系进行了详细介绍，对网络安全与党委工作的关联进行探讨，并表示，党委（党组）应建立和落实网络安全责任制，把网络安全工作纳入重要议事日程，明确工作机构，加大人力、财力、物力的支持和保障力度。

最后，武汉市网络安全协会党支部书记、秘书长刘悦恒总结发言。

刘书记首先代表武汉网安协会感谢汇科智创精心策划，提供了双方党员交流互动的平台，强党建、促交流、谋发展。感慨展厅所见所闻，让协会支部党员了解了汉阳市政 70 年光辉发展历程，希望双方党员同志继续发奋图强，发扬老一辈创业者和共产党员的精神，共同发动更多协会会员单位党组织和党员为城市建设和行业发展贡献力量。希望这样的活动可以长期办下去，为双方共举党建引领之旗，共搭情谊互助之桥，共谋高质量发展之路。

“高举党旗跟党走，百年党史寻初心”走进武昌红巷农讲所

为深入开展学习贯彻习近平新时代中国特色社会主义思想主题教育，弘扬伟大建党精神，传承革命传统，8 月 18 日上午，中共武汉市网络安全协会支部开展“高举党旗跟党走，百年党史寻初心”党建主题活动，在支部书记刘悦恒同志的带领下前往武昌红巷参观了中央农民运动讲习所，学习了解了武昌农讲所的创建过程以及重要意义。

在武昌农讲所旧址纪念馆，党员们肃穆仰望在青瓦灰砖的建筑中央悬挂着醒目的红色牌匾，上有周恩来题写的一行大字“毛泽东同志主办的中央农民运动讲习所旧址”。红色的屋顶，朱黄的墙壁，一排排整体的红木长凳，教室内悬挂的“国民革命成功万岁”等横幅让人一秒穿越回峥嵘年代，在可视可听可触可感中追忆先烈事迹、感受红色情怀，增强党性修养。

通过学习，党员们了解到，中央农民运动讲习所是第一次国共合作时期毛泽东同志倡议创办并主持的一所培养全国农民运动干部的学校，于 1927 年 3 月 7 日在武昌开学。“讲习”一词，“讲”为讲课，“习”则代表军事训练和实践。毛泽东以中共中央农委书记身份，在此亲自授课。1927 年 6 月 10 日，800 多名学员从这里奔向农村，他们像星星之火撒向神州大地，形成了中国革命的燎原之势。1963 年，武昌中央农民运动讲习所旧址纪念馆正式对外开放，现为全国重点文物保护单位，获“全国爱国主义教育示范基地”称号。

这是一座修葺精致的院落，位于武昌红巷 13 号。大门正上方，是周恩来题写的牌匾“毛泽东同志主办的中央农民运动讲习所旧址”。这里也是一处重要的革命文化遗址，除毛泽东外，瞿秋白、恽代英、彭湃、方志敏等都曾在此授课。

星星之火，可以燎原。武昌中央农民运动讲习所旧址，正是这“燎原星火”的迸发之地，而将这革命的火炬传承下去，正是我们共同的伟大使命。

本次党日活动，党员们深受鼓舞，将铭记先辈们的伟大贡献，努力在未来的工作中不断拼搏进取，为实现中华民族伟大复兴的中国梦砥砺前行！

信仰护航 企业党建网络安全防线

■ 彭建军 武汉安恒信息科技有限公司总经理

一、引言

网络安全行业作为当今数字化时代的关键领域之一，承担着维护国家安全、企业信息安全以及社会稳定的重大使命。在这一背景下，党建活动的开展对于企业的可持续发展和国家安全具有重要意义。本文将从我作为企业总经理的角度出发，分享我们企业在党建活动中的经验与体会。

二、党建活动与网络安全行业

（一）行业背景

在充满挑战的网络安全行业中，政治稳定、社会和谐是企业发展的重要基础。党建活动的开展为确保企业在风险中稳健前行提供了坚实的支持。网络安全行业不仅关乎企业的商业利益，还直接涉及国家安全。因此，企业党建活动必须与国家网络安全战略相协调，确保企业的行为与国家战略保持一致，不仅维护企业的长远利益，也为国家的网络安全做出贡献。

（二）党建与企业文化

党建活动有助于构建企业积极向上的文化，强调员工的责任感和使命感，这与网络安全行业要求的高度纪律和责任感相契合。在网络安全行业，每个员工都应该意识到他们的工作不仅仅是为了企业的成功，还关系到国家的安全。因此，企业党建活动应该引导员工树立更高的使命感，将国家网络安全战略融入企业

文化之中。

三、党建实践

（一）党组织建设

我们企业充分利用党组织的作用，建立了稳定的组织结构，确保信息流通畅通无阻。党组织在网络安全行业的作用不可小觑。它不仅是一个纯粹的政治组织，更是一个强大的组织架构，用于促进信息共享和沟通。我们建立了党组织的信息平台，确保党员可以随时分享行业动态、政策变化以及安全威胁信息。这有助于企业更快地响应变化，提高了我们的整体竞争力。

（二）党建与技术创新

网络安全行业在技术创新方面要求持续领先。我们党组织鼓励员工参与技术研发，提升技术水平。党员之间的交流和合作不仅仅是组织间的合作，更是技术领域的创新合作。我们鼓励党员在技术领域分享知识，组织技术讨论和培训，以确保我们始终处于行业的前沿。

（三）党建与企业发展

党建活动的持续开展有助于企业的稳健发展。我们通过建立党建活动的评估机制，确保党建工作与企业战略目标保持一致，取得了显著成果。我们定期对党建活动的成效进行评估，并对不同党组织的表现进行排名，以鼓励各党组织积极参与活动。党建活动的成效与企业的发展息息相关。通过党建活动，我们能更好地了解员工的需求，建立更紧密的员工关系，提升员工忠诚度，减少人才流失，确保企业的长期稳健发展。

四、党建活动的影响

（一）提升企业声誉

在网络安全行业，企业的声誉是至关重要的。由于涉及敏感数据和信息安全，客户更加倾向于与有良好声誉的企业合作。党建活动在提升企业声誉方面发挥了关键作用。首先，党员作为企业的道德典范，他们的行为和决策对企业的声誉产生直接影响。他们的廉洁和诚信形象赢得了客户和合作伙伴的信任。此外，党建活动鼓励党员积极参与社会公益活动，回馈社会，树立了企业的社会责任感。这些举措不仅提升了企业的社会形象，还树立了积极的品牌形象，为企业赢得了更多的客户和合作伙伴。

企业的声誉不仅对业务合作伙伴重要，也在招聘和留住优秀员工方面发挥了作用。有良好声誉的企业更容易吸引人才，员工也更愿意留在一个受尊重和信任的组织中工作。因此，党建活动对企业的声誉提升具有长期和持续的效果。

（二）提高员工凝聚力

员工之间的凝聚力和团队合作精神对于网络安全行业至关重要。这个行业要求员工密切协作，共同应对复杂的网络威胁和攻击。党建活动促进了员工之间的凝聚力和团队合作精神的发展。通过党组织的活动和培训，员工更容易建立紧密的联系，建立起相互信任的关系。党员在这个过程中扮演了积极的角色，他们作为榜样，鼓励其他员工积极参与团队活动和合作项目。

这种凝聚力有助于提高工作效率，团队成员更容易共同追求目标，更好地应对挑战和困难。在网络安全领域，信息共享和紧密协作是至关重要的，党建活动为员工提供了一个分享经验和学习的平台，有助于他们的个人成长和职业发展。员工感到他们是一个紧密团队的一部分，这提高了他们的满意度和忠诚度，降低了员工流失率。

（三）增强安全意识

网络安全行业对员工的安全意识要求极高。党建活动有助于培养员工的安全意识，使他们更加警觉和谨慎。为了应对不断变化的网络威胁和攻击方式，我们通过党组织定期组织网络安全知识培训。这些培训帮助员工了解最新的威胁趋势和攻击技巧，提高了他们的安全意识。

党员在这方面发挥了特殊的作用。他们被视为安全意识的先锋，在日常工作中传播着安全意识。他们鼓励同事养成良好的安全习惯，如定期更新密码、警惕钓鱼邮件等。这种集体的安全意识有助于减少员工的

安全疏忽和错误，降低了社会工程和网络攻击的风险。

党建活动的影响不仅体现在企业内部，还体现在对整个网络安全行业的推动作用。我们的企业通过党建活动树立了行业标杆，成为网络安全行业的典范，为其他企业提供了学习和借鉴的机会。这种积极的示范效应有助于整个行业提升声誉和安全意识水平。

五、党建活动的挑战与应对

党建活动在网络安全行业中虽然有着重要的作用，但也面临一些挑战。下面我将介绍一些主要的挑战以及我们采取的应对措施。

（一）人员流动

网络安全行业竞争激烈，人才流动是一个常见的问题。党组织在不同企业之间可能会面临党员流失的情况。为应对这一挑战，我们鼓励党员在公司内部晋升，提供更多的职业发展机会，同时也建立了联络机制，与其他企业的党组织保持联系，以吸引更多的优秀人才加入我们的企业。

（二）党建活动的长期性

党建活动是一个长期性的工作，需要持续投入资源和精力。在网络安全行业，业务变化快，党组织需要不断调整工作重点，确保与企业发展保持一致。我们建立了党建活动的规划和执行机制，确保党建工作不因短期变化而受到影响，保持稳定性和持续性。

（三）党建活动与业务需求的平衡

党建活动的开展需要消耗一定的人力和资源，与企业的日常运营和业务需求存在竞争关系。我们通过建立明确的党建工作计划，确保党建活动与业务需求的平衡。党组织的活动必须与企业战略保持一致，以确保资源的最优化利用。

六、结语

党建活动在网络安全行业中扮演着重要的角色，对于企业的稳健发展和国家安全具有不可替代的作用。通过党建活动，我们的企业不仅在业务上取得了显著的成绩，还在员工凝聚力、安全意识和社会责任感方面取得了积极的变化。然而，党建活动仍然面临一些挑战，需要不断调整和改进。

在未来，我们将继续加强党建活动，保持党组织的活力，确保党员积极参与，并与国家网络安全战略相协调。我们将继续为员工提供发展机会，加强安全意识培训，提高员工的综合素质。同时，我们也将继续弘扬企业的社会责任感，积极参与社会公益活动，为社会做出更多的贡献。

党建活动是网络安全行业的一项重要工作，对于企业和国家具有重要意义。通过不断努力，我们将确保党建活动的成功，为企业的可持续发展和国家的网络安全贡献更多的力量。感谢您对党建工作的支持和关注。

坚持总体国家安全观 筑牢网络安全屏障

——访武汉大学国家网络安全学院党委书记、二级教授赵波

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。当前，以网络化、数字化为代表的新科技革命和产业变革深入发展，给国家安全治理带来深刻影响。

网络安全是国家安全体系的重要组成部分，已成为信息时代国家安全的战略基石。我省正在加快建设全国构建新发展格局先行区、奋力建成中部地区崛起重要战略支点，网络安全屏障是重要保障。

如何准确认识网络安全的重要性？如何树立正确的网络安全观？如何筑起网络安全的钢铁长城？9月底，湖北日报全媒记者专访了武汉大学国家网络安全学院党委书记、二级教授赵波。

网络安全“牵一发而动全身”

问：网络安全是国家安全体系的重要组成部分，一旦网络安全这个“神经系统”出问题，将严重影响国家安全和国家发展。面对新形势新任务，如何正确认识和准确把握网络安全及其重要性？

答：网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性、真实性和可控性的能力。

网络安全为何重要？当今时代，网络安全和信息化对一个国家很多领域都是牵一发而动全身的，网络安全已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，广大人民群众的利益也难以得到保障。从世界范围看，网络安全威胁和风险日益突出，并向政治、经济、文化、社会、生态、国防等领域传导渗透。网络安全已经成为我国面临的最复杂、最现实、最严峻的非传统安全问题之一。

网络安全有以下几点作用：

第一、保护个人信息。网络安全能够有效地保护个人信息，防止个人信息被滥用。网络犯罪分子经常利用钓鱼网站、恶意软件、社交工具等手段获取他人的个人信息。这不仅可能造成财产损失，还可能威胁到个人隐私。

第二、避免经济损失。网络攻击可能会导致直接的经济损失。例如，网络诈骗、钓鱼攻击、勒索软件等都可能造成严重的经济损失。企业也可能因为数据泄露或网络瘫痪而遭受巨大的经济损失。

第三、维护社会秩序。网络安全不仅关乎个人和企业，也关乎整个社会的稳定和秩序。网络攻击可能会破坏基础设施、金融系统、交通系统等关键领域，造成社会混乱。

第四、推动信息化建设。网络安全是信息化建设的基础。只有当网络安全得到保障，人们才能放心地

享受信息化带来的便利。

维护网络安全是全社会共同的责任

问：维护网络安全是每个公民义不容辞的责任。很多时候，一些网民不自觉的行动就会触犯法律，就有可能侵犯到他人的个人权益，甚至国家利益。面对纷繁复杂的网络世界，如何树立正确的网络安全观？

答：要充分认识网络安全工作在党和国家事业全局中的重要地位，清醒认识网络安全工作面临的严峻形势，增强维护网络安全的责任意识。

一是网络安全是整体的而不是割裂的。在信息时代，网络安全对国家安全牵一发而动全身，同许多其他方面的安全都有着密切关系。

二是网络安全是动态的而不是静态的。网络变得高度关联、相互依赖，网络安全的威胁来源和攻击手段不断变化，需要树立动态、综合的防护理念。

三是网络安全是开放的而不是封闭的。只有立足开放环境，加强对外交流、合作、互动、博弈，吸收先进技术，网络安全水平才会不断提高。

四是网络安全是相对的而不是绝对的。没有绝对安全，要立足基本国情保安全，避免不计成本追求绝对安全。

五是网络安全是共同的而不是孤立的。网络安全为人民，网络安全靠人民，维护网络安全是全社会共同的责任，需要政府、企业、社会组织、广大网民共同参与，共筑网络安全防线。

完善综合治理，守牢互联网阵地

问：网络空间不是“法外之地”。网络空间同现实社会一样，既要提倡自由，也要保持秩序。如何完善

综合治理，筑牢网络安全屏障？

答：网络空间是虚拟的，但运用网络空间的主体是现实的，大家都应该遵守法律，明确各方权利义务，坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。

第一、制定健全法律法规。国家应制定和完善相关的网络安全法律法规，明确网络安全的基本要求和责任分工。法律法规的制定应涵盖网络安全的各个方面，包括网络基础设施的安全、数据保护、个人隐私保护和网络犯罪的打击等；政府的监管职责、企事业单位的安全管理责任、个人的自我保护责任等，明确违法行为的处罚和法律责任。在立法过程中，需要充分考虑各方的利益和需求，平衡安全和发展的关系，以推动网络安全的持续改善。

第二、加强技术能力和人才培养。建立系统的教育和培训计划，包括网络安全相关的学位课程、职业培训和认证计划。这些计划可以涵盖网络安全的理论知识、技术实践和应用技能，培养专业的网络安全人才；鼓励学术界开展网络安全的研究和创新工作。设立研究基金和奖励机制，支持创新项目和高水平的学术研究。促进学术界与产业界的合作，加强技术转移和应用；建立行业联盟、协会和技术社区，促进网络安全领域的合作和交流。网络安全领域需要综合技术、法律、管理和沟通等各方面的能力，因此应注重培养综合素质和跨领域的人才；加强与国际组织、机构和专家的合作和交流。参与国际标准制定、信息共享和联合研究项目，借鉴国际先进经验，提升我国网络安全的技术能力和人才培养水平。

通过以上措施，可以加强技术能力和人才培养，培养更多专业的网络安全人才，满足不断增长的网络安全需求，并推动网络安全领域的发展和创新。

第三、提高公众网络安全意识。开展网络安全教育和培训活动，包括在学校、企事业单位、社区等场所开展网络安全知识的普及和培训。教育公众有关网络威胁、常见网络攻击方式、个人信息保护等方面的知识，提高他们对网络安全的认识和理解。通过各种渠道，如主流媒体、社交媒体、户外广告等，开展网络安全宣传活动。宣传网络安全的重要性，提醒公众注意网络风险和安全隐患，并提供简单实用的网络安全建议。为公众提供网络安全指南和操作手册，包括如何设置强密码、避免点击垃圾邮件、安全使用社交媒体等。这些指南可以以易懂的方式解释网络安全概念和最佳实践，帮助公众采取有效的安全措施。组织网络安全活动，如网络安全讲座、研讨会和比赛等。通过这些活动，向公众展示网络安全的重要性，提供实际操作经验，并促进公众之间的交流和分享。向公众提供安全工具和资源，如杀毒软件、防火墙、加密工具等。同时，向公众推荐可信赖的网络安全信息来源和网站，让他们可以获取最新的网络威胁信息和防护建议。与政府、教育机构、企业和非营利组织等建立合作机制，共同推动网络安全意识的提高。通过共同努力，能够更广泛地传播网络安全知识，覆盖更多的人群。定期公布网络安全案例，分析其原因和教训，警示公众避免类似的安全漏洞和陷阱。这样的案例分析可以提高公众对网络安全风险的警觉性。通过以上方法，可以提高公众对网络安全的意识，增强他们在日常网络使用中的安全意识和自我保护能力。加强国际间的网络安全合作与信息共享，共同应对跨国网络威胁。与其他国家、国际组织和企业建立合作机制，分享经验、技术和情报，共同应对网络攻击和网络犯罪。

第四、加强监管和执法力度。建立健全的网络安全监管机制，对违法违规行为进行打击和惩处。加强执法力度，对网络攻击、数据泄露和网络犯罪行为进行严厉打击，形成对违法行为的威慑效应。

网络安全综合治理需要多方合力，涉及政府、企业、学术界和公众等各方的积极参与和配合。只有通过综合治理，才能够筑牢网络安全的屏障，保障国家和个人的网络安全。

文章来源：湖北日报

湖北日报全媒记者 江卉 实习生 王莹莹


副会长单位
湖北珞格科技发展有限公司
锐意进取 大爱无疆
黄凯先生
武汉大学客座教授
珞格科技董事长
珈格文化艺术中心董事长
珞格生态农业董事长

黄凯先生

1962 年出生于湖北

毕业于中山大学历史系，诚信企业家、慈善家、卓越投资人

湖北珞格科技发展有限公司董事长

湖北珞格生态农业发展有限公司（湖北珞格小镇）董事长

湖北珞珈文化艺术中心（珞格美术馆）董事长

黄凯先生有着卓越的投资眼光，2015 年，黄凯创立珞格科技，正式宣告进入网络安全领域。

2018 年 3 月 19 日，黄凯向武汉大学网络安全学院捐赠 200 万元，设立“珞格天佑奖学金”，这是武汉大学网安学院成立后设立的第一支奖学金，专门用于培育优秀网安人才，为网络安全事业注入新鲜血液，孕育中坚力量提供一份他的力量。

2020 年 10 月，黄凯与武汉大学“再续前缘”，在湖北省委网信办的支持下，联合湖北省网络空间安全研究中心、武汉大学国家网络安全学院共建“网络空间安全联合实验室”，专注于云计算、大数据、可信、工控等方面的网络安全问题研究，建立自主创新平台，吸纳众多信息安全领域专家、学者积极开展安全前沿领域的研究。

同时为了吸引国内顶尖人才，特聘请武汉大学武汉校友会计算机分会会长，前武汉大学计算机学院院长，软件工程国家重点实验室教授、主任，国家级教学名师、网络安全学院教授何炎祥教授为实验室主任，为实验室的发展、优秀青年人才的挖掘和培养保驾护航，

黄凯对人才的重视，使得其身边聚集了一大批志同道合的网安人在逐梦的路上一同披荆斩棘。在珞格的

精英团队中，50% 安全技术人员具备 10 年以上网络安全行业工作经历，拥有来自 IT 架构、网络、主机、数据库、渗透测试、风险评估、等保测评、商用密评等全方位安全专业领域的复合型人才。

在 2023 年 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”！作为武汉市网络安全协会副会长单位，珞格科技凭借过硬的综合实力以及雄厚的技术实力从 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。

在 2023 年 7 月由国家密码管理局组织的商用密码应用安全性评估（简称密评）从业人员资质考试中更是取得了湖北省通过率、通过人数双第一的优异成绩。

目前珞格科技已经发展成为具有网络安全等级测评与检测评估机构服务认证资质、ISO9001 质量管理体

系认证、ISO27001 信息安全管理体系认证、ISO20000 信息技术服务管理体系认证、ISO14001 环境管理体系认证、ISO45001 职业环境健康管理体系认证、ISO27701 隐私管理体系认证、CCRC 信息安全风险评估服务资质、CCRC 网络安全审计服务资质、CCRC 信息系统安全运维服务资质、CCRC 信息安全应急处理服务资质、CMMI3 级资质、ITSS 信息技术服务标准运行维护资质、CNAS 机构认可等多项专业资质的综合型网络安全服务企业。

凭借着强大的人格魅力和优秀的领导能力，黄凯带领着他的团队已将他“质量为先、信誉为重、管理为本、服务为诚”的安全服务价值理念带给了湖北、广东、浙江、山西、海南、河南、河北、四川、宁夏、湖南、广西、辽宁、江西、贵州、重庆、福建等十余个省份的上千家客户。

黄凯在践行他作为一个网安人理想的同时，更是一位有着红色革命情怀，根红苗正的红色子弟。他拥护共产党，骨子里流淌着的“红色”血液。近年来，黄凯一直坚持着慈善事业，助力教育，资助贫困学子，为无数学子送去光明，多年来已经累计捐助超过 100 万元。

而在 2020 年湖北的至暗时刻。黄凯先生动员旗下的珞格商用设备公司员工放弃休假，不畏艰险，全力投入到消毒剂的生产供给工作中。同时，又多方调配资源，积极联系各大医院、各省医疗队以及武汉地区街道办等抗疫中心，捐赠应急救援物资总价值超 1000 万元，有效缓解了疫情爆发以来各大医疗机构和单位部分防控物质紧缺的压力，彰显了其对自身肩负的社会责任的认识与担当。

黄凯表示，未来，他将继续活跃在网安事业中、公益前线上，发光发热，以追寻梦想，实现自我价值为初心，续写新的传奇故事。

新时代背景下，我国《网络安全法》实施回顾与展望

■ 朱超 泰和泰律师事务所律师

摘要：新时代背景下，全球已经步入信息化时代，展现了全新的社会阶段。推进互联网建设，就是一个重要内容。自我国 2017 年 6 月 1 日正式施行《网络安全法》，对保护个人信息、治理网络诈骗、保护关键信息基础设施、网络实名制等方面作出规定，成为我国网络空间法治化建设的重要里程碑。

党的十八大以来，以习近平同志为核心的党中央高度重视网络安全工作，习近平总书记多次发表重要讲话、作出重要指示批示。习近平总书记从党和国家事业发展全局的高度对网络安全工作作出一系列新部署新要求，加强网络安全工作战略谋划和顶层设计，推动相关立法不断完善，形成了以网络安全法为核心、基础与框架，数据安全法、个人信息保护法等法律为支柱，各级各类法规、规章为配套的系统化、综合性、全覆盖的网络安全法律体制，对保障网络安全与秩序，维护网络空间主权和国家安全，保护公民、法人合法权益，促进经济社会健康发展，发挥了巨大作用[1]。在中国式现代化新征程全面开启的关键节点，回顾与展望《网络安全法》的实施，思考如何进一步发挥网络安全法治对实现中国伟大复兴的保障作用，具有关键意义。

一、网络安全领域法治化建立

近十余年来，我国在网络安全法治建设中不断探索，相继颁布《网络安全法》、《数据安全法》、《个人信息保护法》等法律法规及相关规定，同时还颁布《互联网新闻信息服务管理规定》、《区块链信息服务管理规定》、《网络信息内容生态治理规定》等部门规章，大约 100 余部。其中，《网络安全法》具有关键性、开创性意义，其出台意味着我国网络安全事业步入了规范治理的法治化轨道。[2]

我国稳步建立以《网络安全法》为核心的网络空间安全法治体系。配套文件如《关键信息基础设施安全保护条例》、《网络产品安全漏洞管理规定》、《网络信息内容生态治理规定》、《网络安全审查办法》等行政法规、部门规章、部门规范性文件紧随其后，构建了覆盖各效力位阶的网络安全法律法规体系，涉及保障网络运行安全、网络设备设施安全、数据和个人信息安全以及网络信息内容安全等各方面，为《网络安全法》的贯彻落实和网络空间安全保障，提供了全方位、立体化的支撑。[3]

二、数据安全和个人信息保护成为网络安全治理

[1] 筑牢网络空间安全屏障——党的十八大以来网络安全工作综述_央广网 (cnr.cn)

[2] 黎慈，社会分层视野下网络安全立法体系的构建【J】，湖北社会科学，2019（05）：125-131

[3] 黄道丽，《网络安全法》实施五年回顾与展望【J】，网络空间战略论坛，2023（02）：61-64

领域重点

随着信息技术和人类生产生活交汇融合，各类数据迅猛增长、海量聚集，对经济发展、人民生活都产生了重大而深刻的影响。数据安全已成为事关国家安全与经济社会发展的重大问题。党中央对此高度重视，就加强数据安全工作和促进数字化发展作出一系列部署。中央全面深化改革委员会第二十六次会议强调，我国具有数据规模和数据应用优势。

2021 年 9 月 1 日，《数据安全法》正式施行。数据安全正式确立法治化规制路径。《数据安全法》明确了总体国家安全观的立法目标，重点聚焦数据安全层面的突出问题，确立了数据分类分级管理，建立了数据安全风险评估、监测预警、数据安全审查等基本制度，并明确了相关主体的数据安全保护义务，这是我国首部数据安全领域的基础性立法。

数据安全法为公安机关全链条打击网络电信诈骗、严厉惩治侵犯公民个人信息、单位或个人倒卖数据等违法犯罪行为提供了关键的法律保障，这更加有利于落实网络安全等级保护制度，全方位保护个人信息安全。

2021 年 11 月 1 日，《个人信息保护法》正式施行，标志着我国个人信息保护立法体系进入新的阶段。该部法律明确规定了，不得过度收集个人信息、大数据杀熟，对人脸信息等敏感个人信息的处理做出规制，完善个人信息保护投诉、举报工作机制等，充分回应了社会关切，为破解个人信息保护中的热点难点问题也提供了强有力的法律保障。

《个人信息保护法》提供的个人信息保护路径并不局限权利与义务的一致性要求，还包括专门的国家机关履行个人信息保护职责，提供全方位的个人信息保护和救济方式。一方面，《个人信息保护法》规定国家机关处理个人信息同样应当遵守法律、行政法规规定的权限和程序。个人信息权益受到前所未有的重视，即使国家机关是个人信息处理者，其收集处理范围和限度也不得超出履行法定职责之需要。并且，国家机关处理个人信息之前，应当依照规定，履行告知义务。另一方面，《个人信息保护法》明确规定了国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。国务院有关部门依照本法和有关法律、行政法规的规定，在各自职责范围内负责个人信息保护和监督管理工作。[4]

三、网络安全领域监督检查愈发强化，执法工作成效显著

自“庆祝新中国 70 华诞”到“庆祝中国共产党成立 100 周年”，各项重大活动期间的网络安全工作圆满完成安全保障任务。近些年，网络安全主管监管部门推动网络安全行政执法规则制定，加快建设执法队伍和执法能力，依法开展网络安全监督检查，网络安全执法逐渐走深走实，违法违规问题得以有效惩处。

（一）侵犯公民个人信息

1、团伙利用社保系统漏洞，非法获取公民个人信息

2022 年 12 月 7 日，四川省南充市公安局侦破一起侵犯公民个人信息案件，抓获犯罪嫌疑人 121 人，查获公民个人信息 2300 余万条，发现国内多地各类信息系统平台漏洞 300 余个，收缴黑客工具 12 套。

2、最高人民检察院发布检察机关落实“七号检察建议”典型案例

男子利用从事寄递客服的便利条件，伙同妻子查询、出售大量寄递用户的个人信息牟利，非法获利 24 万余元，两人双双获刑。

3、涉及 27 个省份的特大系列侵犯公民个人信息案件

2022 年 9 月 22 日，鸡西市公安局侦破特大侵犯公民个人信息案件，共抓获犯罪嫌疑人 322 名，依法扣押涉案资金 560 余万元，扣押电脑 78 部，手机 412 部，涉案银行卡 638 张。

（二）数据泄露事件

1、河南一高校学信网信息泄露

[4] 专家解读 | 《个人信息保护法》：构筑新时代个人信息权益保护的安全防护网 _ 中央网络安全和信息化委员会办公室 (cac.gov.cn)

2022 年 8 月 28 日，校学生会学生干部参加社会实践活动时，应郑州泽梦企业管理咨询有限公司业务人员要求，擅自组织学生参与网上《信师宿舍满意度调查问卷》活动。经核实，确实存在部分学生学信码被盗用情况，造成学生在三个月内不能享受购买苹果平板电脑、耳机等产品的优惠政策。

2、B 站 2.2 亿余条用户 ID、手机号疑被出售

2022 年 7 月 6 日，一张在暗网叫卖 2.2 亿余条 B 站用户信息的截图在网上流传，泄露数据疑似包括用户账号（UID）和手机号，价格为 0.5 比特币或 17.72 以太币。

3、丰田或泄露近 30 万客户信息

2022 年 10 月 7 日，丰田汽车发现，296019 名客户的电子邮件地址和客户编号可能已被泄露。不过，其他敏感个人信息如姓名、电话号码和信用卡信息等均未受到影响。

4、蔚来汽车用户数据泄露，被勒索 225 万美元比特币

2022 年 12 月 11 日，蔚来公司收到外部邮件，声称拥有蔚来内部数据，并以泄露数据勒索 225 万美元（当前约 1570.5 万元人民币）等额比特币。

（三）重点查处严重违法违规平台，形成有效震慑

国家网信办指导各级网信部门，综合运用执法约谈、责令整改、处置账号、移动应用程序下架、暂停功能或更新、关闭网站、罚款、处理责任人、通报等多种处置处罚手段，对严重违反有关互联网信息内容管理法律法规的网站平台，依法予以严处。

针对新浪微博及其平台账号屡次出现法律、法规禁止发布或者传输的信息的问题，国家网信办负责人依法约谈新浪微博主要负责人、总编辑，责令其立即整改，严肃处理相关责任人。北京市网信办对新浪微博依法予以罚款的行政处罚。

针对豆瓣网及其平台账号屡次出现法律、法规禁止发布或者传输的信息的问题，国家网信办负责人依法约谈豆瓣网主要负责人、总编辑，责令其立即整改，自行暂停相关跟评功能和更新，严肃处理相关责任人。北京市网信办对豆瓣网依法予以罚款的行政处罚。

针对微信对用户发布的信息未尽到审核管理义务、多个微信公众号传播涉历史虚无主义等有害信息的问题，广东省网信办依法约谈微信负责人，责令其立即整改，处置相关账号，从严处理责任人，并对微信依法予以罚款的行政处罚。

针对百度贴吧出现法律、法规禁止发布或者传输的信息的问题，北京市网信办依法约谈百度公司相关负责人、百度贴吧主要负责人，责令其限期整改，自行暂停百度贴吧及其应用程序新用户注册功能，从严处理相关责任人，并对百度依法予以罚款的行政处罚。

针对知乎网跟评环节存在法律、法规禁止发布或者传输的信息的问题，国家网信办指导北京市网信办依法约谈知乎网负责人，责令其立即整改，自行暂停跟评功能，严肃处理相关责任人，并对知乎网依法予以罚款的行政处罚。

针对金山毒霸应用程序弹窗推送诋毁革命烈士邱少云内容，国家网信办指导北京市网信办依法对其主办方负责人进行约谈，责令立即停止违法行为，暂停弹窗信息推送功能，进行全面深入整改，从重处理有关负责人，并依法予以罚款的行政处罚。

针对京东、拼多多、淘宝等 3 家电商平台售卖涉儿童邪典内容的儿童服装等商品破坏网络生态的问题，北京市、上海市、浙江省网信办分别对 3 家平台予以约谈，责令其全面排查违法有害信息，并分别予以罚款的行政处罚。[5]

四、依法保障经济社会发展与公民合法权益

网络安全与社会公共利益、公民合法权益紧密相联系。我国加强网络安全领域重点建设，具有促进和保障经济社会健康发展的重要意义。

在这方面，网络安全法奠定了数据信息安全与个人信息保护的法律基础，并由数据安全法与个人信息

[5] 2022年全国网络执法取得显著成效-中共中央网络安全和信息化委员会办公室 (cac.gov.cn)

保护法予以具体保护。随着《数据安全法》、《个人信息保护法》相继实施，各级网信部门依法开展数据安全、个人信息保护等领域执法。针对滴滴企业版等 25 款移动应用程序存在严重违法违规收集使用个人信息问题，依法通知应用商店下架相关应用，要求相关运营者严格按照法律要求，参照国家有关标准，认真整改存在的问题，保障广大用户个人信息安全。针对“美原油”“链工宝”“快输入法”等移动应用程序存在违法收集使用个人信息问题，依法对其采取下架处置措施。针对“伴圈”“AI 换脸相机”等多款新技术新应用未经评估上线且存在风险的移动应用程序，依法予以下架处置。[6]

目前，我国网络安全领域法治建设还在不断完善推进之中。2022 年 9 月，国家网信办公布了关于修改网络安全法的征求意见稿，建议进一步加强对危害网络运行安全、信息安全和关键信息基础设施行为的处罚力度，为网络安全构筑更坚固的屏障。相信在党中央的坚强领导下，我国网络安全法治建设必将迎来新的春天。

[6] 黄道丽，《网络安全法》实施五年回顾与展望【J】，网络空间战略论坛，2023（02）：61-64

作者简介：泰和泰律师事务所朱俊超律师自 2017 年毕业执业至今，具备英语和法律双重知识背景，在刑事辩护、企业企业合规、数据合规、公司商事争议解决等方面具有一定的经验，曾为湖北省司法厅、武汉市住房保障和房屋管理局、武昌区司法局、东风日产汽车有限公司等提供法律服务。

新华网：武汉市 2023 年国家网络安全宣传周启动仪式举行

9 月 11 日，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启动仪式暨“武汉以我为荣 • 文明上网篇”发布活动举行。活动由武汉市委宣传部、市文明办、市委网信办主办。

此次宣传周活动时间为 9 月 11 日至 9 月 17 日，将通过举办“黄鹤杯”网络安全人才创新大赛、网络安全进基层、长江灯光秀等一系列活动，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。

据悉，近年来，武汉市将国家网安基地建设与超大城市治理有机结合，科学构筑网络安全人才技术产业生态，积极探索构建超大城市网络安全防御体系。自 2016 年起，武汉市已连续 8 年举办国家网络安全宣传周活动，发动各方力量广泛参与网络安全宣传教育。

文章来源：新华网

构筑汽车信息安全防线智能汽车网络安全讲堂在武汉经开区举行

远程入侵、恶意控制、数据泄漏……聚焦车联网网联安全热门话题。9 月 14 日，2023 年武汉网络安全公益行“智能汽车网络安全大讲堂”在岚图汽车科技有限公司举行。

此次论坛由武汉市委网信办指导，武汉经开区工委网信办、武汉市网络安全协会共同主办，岚图汽车等单位承办，是“2023 年国家网络安全宣传周”的重要活动之一。

现场，岚图汽车、武汉大学国家网络安全学院、武汉市网络安全协会、天融信科技集团等四方代表，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。

近年来，武汉经开区积极对接国家智能网联汽车重大战略布局，抢占智能网联汽车新赛道。一批智能网联汽车产业链上下游企业加速聚集，形成了从硬件生产到示范运营的全产业链生态，覆盖自动驾驶方案、车路协同、智能座舱等多领域。随着“智能网联 + 汽车”应用范围变广，数据安全、隐私保护等问题日益引发关注。

现场，岚图汽车网络安全高级专家刘翀分享了岚图汽车在智能汽车安全上的探索和实践。除“云管端”一体化的纵深防御安全架构外，岚图汽车还配置“一键隐私”功能，从根本上杜绝数据泄密的可能性。

时下，智能网联汽车已成为汽车行业数字化的加速器，产品和技术还在不断进化，相关配套法律法规和标准也在不断完善中。在场学者专家代表纷纷呼吁，规避智能网联汽车网络攻击和安全风险，不仅需要整车企业加强汽车车载系统自身的安全建设，还需要智能网联汽车上下游企业各方努力，共同打造汽车行业网络安全共建共治共享治理新模式。

出品：武汉经开区工委宣传部
武汉经开区融媒体中心
采写：记者王双双 摄影肖怡珂 吴世安
编辑：吕作璐 蒋秋雨

【安恒】

践行网络安全责任，提升全名网络安全意识

2023 年国家网络安全宣传周于 9 月 11 日在福州海峡国际会展中心盛大开幕。作为网络安全行业的领军企业之一，安恒信息已是连续十届参与网络安全宣传周。本届安全周，安恒信息特邀请武汉市汉阳区委国安委、区委网信委成员单位、区其他重点单位、区部分企业和卫健系统等单位，在武汉安恒信息科技有限公司安全创新体验中心展示了网络安全领域的创新成果与责任担当，为公众揭示了一个又一个网络安全的“硬核”实力。

安恒信息在本届宣传周期间继续拆解网络诈骗套路，以提升公众的反诈意识。这是安恒信息连续十年参与国家网络安全宣传周的重要举措之一，持续助力提高人民的反诈意识，用科技力量保障国家与人民的网络安全。

此次活动邀请到安恒信息网络安全专家王佳带领大家提高日常网络安全防护意识。介绍网络安全已经上升到国家层面，网络空间是“第五空间”，是国家主权的新疆域。引用国内外典型网络安全事件，武汉地震监测中心遭网络攻击事件，西北工业大学遭美国 NSA 网络攻击事件，美国最大燃油管道被“掐断”事件。并分享实际工作生活中如何保护好个人隐私的小妙招，加强个人密码管理，注意日常用网安全，养成良好的安全习惯。

活动邀请到中国电信天翼安全科技有限公司蒋瑾讲述勒索病毒与网络钓鱼防范。2023 年调查报告分析显示，随着安全技术的不断提高，“钓鱼”、“勒索”两大重点安全事件占整体网络安全事件的比例越来越高，如何防范这两大安全事件已经成为各大机关单位安全部门关注的工作要点。基于勒索病毒加密信息难以恢复攻击来源难以追踪的特点，蒋瑾为大家介绍了常见勒索病毒的种类、主要类型、传播方式、攻击流程、判断方式、防范要点及具体案例分析。同时蒋瑾为区分了“网络钓鱼”的常见方式、常见场景、8 大迹象及防范意识。

在接下来的一周中，安恒信息将继续参与网络安全协同治理论坛、网络安全服务产业发展分论坛、网络安全标准与实践论坛等多个论坛和研讨会，分享成功经验，探讨网络安全领域的未来发展趋势和创新方向。

在 2023 年国家网络安全宣传周中，安恒信息展示了公司在各个领域的创新成果与责任担当。这不仅体现了公司在网络安全领域的领先地位和影响力，更展示了公司积极推动网络安全事业发展的决心和行动。未来，安恒信息将继续致力于网络安全领域的技术研发和应用实践，为保障国家和人民的网络安全做出更大的贡献。

【天融信】

安全出行，网络护航

2023 年国家网络安全宣传周于 9 月 11 日 -17 日，在全国范围内统一举办。湖北天融信网络安全技术有限公司（以下简称湖北天融信）作为武汉市网络安全协会副会长单位，积极参与开展网络安全公益宣传活动，以通俗易懂、百姓喜闻乐见的方式，宣传网络安全理念、普及网络安全知识、推广网络安全技能，推动全社会网络安全意识和防护技能的提升，开展系列宣传活动，承担协会副会长单位的工作职责和使命。

经过精心筹备策划和多轮沟通，湖北天融信代表武汉网络安全协会同武汉地铁集团有限公司达成活动合作意向，并于 2023 年 9 月 14 日下午 2 点 30 分，在武汉地铁集团会议大厅开展 2023 年武汉市国家网络安全宣传周——网络安全进基层专家宣讲活动，武汉地铁集团相关领导对此活动高度重视，组织下属股份公司、运营公司、土地公司、设计公司、修理公司、党群部、技术中心、桥隧公司、建设公司、拆迁公司等十余家分支机构共 80 余人参加。湖北天融信组织本单位专家讲师从战略意义、法律法规、实时案例、注意事项等多角度全方位向武汉地铁集团开展了网络安全意识培训，现场组织了简单的问答环节，发放宣传物料，加深基层人员对网络安全意识的印象，提升一线人员网络安全防护意识和水平，活动最终取得良好效果。

【东方网盾】

共建网络安全，共享网络文明

在“网安周”期间，东方网盾通过线上线下相结合的模式开展公益宣传活动。

线上宣传：员工内宣

东方网盾通过公众号等平台发布科普文章及宣传海报，员工们积极转发网络安全知识宣传手册，并向家人、朋友普及网络安全知识，用切实行动凝聚“网络安全为人民、网络安全靠人民”的思想共识。

线下宣讲：深入企业

东方网盾深入武汉市水务集团、十堰武当山机场等单位进行网络安全意识宣教会，列举电信诈骗、钓鱼邮件等案例，采用知识竞赛等形式，激发职工们树立网络安全意识，引导职工们掌握网络安全常识和日常防范重点。

东方网盾本次公益活动获得好评如潮。未来，东方网盾将继续承担企业的社会责任，为国家网络保驾护航！

【同德兴】

网络安全进校园，争做安全小卫士

2023 年 9 月 11 日 -9 月 17 日是第十个国家网络安全宣传周，武汉同德兴积极配合武汉市网络安全协会举行了一周的网络安全宣传周进校园公益活动，在武汉光谷外国语学校、武汉市光谷第十六小学、新洲区实验中学、新洲区邾城街中心小学、武汉市第六十四中学、硚口区博学小学给全体师生宣讲，活动主题为”争做网络安全小卫士”，期间以有趣的互问互答形式来讲述网络的优缺点，让学生结合实际讲述自己的观点，共讲述了三个关于网络危

害的案例来引起学生对网络安全的重视，告诫学生注意网络信息安全，提高自我防范意识，学习网络自我保护的方法，最后还有一些随堂小测试来增加学生记忆点。此次活动同德兴积极投身到投身武汉市网络安全宣传工作中让学生师生认识到了维护网络安全不仅是国家的事情，而是大家小家千万家的事情，人人都要为此贡献出一份自己的力量，来共同维护我们这个”大家”，一起勇担社会责任。

【安域】

百家齐放，安域亮点频出

党的十八大以来，我国网络安全和信息化事业取得重大成就，党对网信工作的领导全面加强，网络空间主流思想舆论巩固壮大，网络综合治理体系基本建成，网络安全保障体系和能力持续提升，网信领域科技自立自强步伐加快，信息化驱动引领作用有效发挥，网络空间法治化程度不断提高，网络空间国际话语权和影响力明显增强，网络强国建设迈出新步伐。

——2023 年 7 月 15 日习近平对网络安全和信息化工作作出重要指示强调

9 月 11 日至 17 日，以“网络安全为人民，网络安全靠人民”为主题的 2023 年国家网络安全宣传周（以下简称“网安周”）在全国范围内统一开展，通过形式多样、内容丰富的系列活动，宣传网络安全理念、普及网络安全知识、推广网络安全技能，营造全社会共筑网络安全防线的浓厚氛围。网安周期间，武汉安域通过网络安全讲座、网络安全知识竞赛答题、网络安全进基层等多种方式深入开展宣传教育活动，手握数字盾牌，勇“网”直前。

亮点一：教培输出 播尽网安之种

网安周期间，武汉安域网络安全专家深入各地，围绕网络安全法律法规解读、综合防护体系介绍、网络安全意识强化、网络安全风险分析等内容，为多家关键信息基础设施重要行业举办数十场相关专题讲座。不懈的宣传，播下一颗颗茁壮的种子，让网络安全深入人心、落到实处。

亮点二：以赛促学 浇灌网安之花

9 月 14 日至 17 日，武汉安域技术专家为多家武汉市头部医院部署开展网络安全演练、网络安全知识竞答等活动，并安置宣传展板及手册展示。线上线下多形式内容相结合，帮助从业人员激发兴趣、提高技能，深刻理解网络安全的核心概念。

亮点三：践行责任 缔结网安之果

9 月 11 日，武汉安域紧跟武汉市“网络安全七进”系列行动，参与华润电力华中公司和武汉天然气集团的网络安全宣传工作，针对重点单位宣传网络安全理念、普及网络安全知识，推广网络安全技能，推动网络安全意识和防护技能提升。

2023 年国家网络安全宣传周已落下帷幕，但武汉安域的网络安全宣传工作始终在路上。网信工作的使命重大，新时代新征程下的网信事业高质量发展，在建设网络强国的行动指南之下，武汉安域将全力承担好国家交办的政治任务，紧跟行业主管部门工作要求，优化技术团队，用心服务用户，为护航数字中国贡献安域力量。

【绿盟】

筑牢网络安全防线 守护信息时代未来

为全面落实党中央、国务院对我国网络安全和信息化的战略部署，进一步增强员工网络安全意识，在国家网络安全宣传周期间，作为武汉市网络安全宣传周活动志愿者单位，绿盟科技于2023年9月8日走进武汉农村商业银行，面向金融后台中心全体人员开展了主题为“落实主体责任，筑牢网络安全防线”的国家网络安全宣传活动，通过专业讲座方式，从身边的意识安全、工作的信息安全、国家信息安全事件分析、网络安全法介绍、信息安全防范指范等方面，结合生活、工作中常见的各类实际事例，让大家充分了解了网络信息安全在身边、了解了网络安全对生活、工作的重要性，通过体验小游戏、快问快答等互动环节让大家在轻松的环境中，深度参与到网络安全这一严肃主题活动当中。

活动期间，宣传周志愿者单位人员通过设立宣传台、悬挂宣传标语、发放宣传折页、现场讲解及播放视频、互动游戏等形式，向参与人员广泛宣传、普及网络安全知识，介绍宣传周中各类网络安全案例，进一步优化金融服务环境，提升金融从业者的网络安全素质和水平。

【泰和泰】

增强法律意识 筑牢安全防线

9 月 14 日上午及 9 月 15 日下午，在网络安全宣传周浓厚的宣传氛围中，泰和泰（武汉）律师事务所网络安全法律服务团队来到武汉市总工会和市联通公司，带来了两场别开生面的网络安全普法“公开课”。

党的十九大将“坚持全面依法治国”作为坚持和发展中国特色社会主义的一条基本方略。近年来，随着网络安全立法不断完善，泰和泰（武汉）律师事务所组建了专业的网络安全法律服务团队，作为武汉市网络安全协会的会员单位和战略合作伙伴，积极参与协会组织的各项活动，为普及网络安全法律法规、解决各项涉及网络安全的法律问题贡献自己的力量。本次网络安全宣传周的主题是“网络安全为人民，网络安全靠人民”，围绕着这一主题，团队的李怀志律师结合生动鲜活的案例和工会工作实际，对于关键信息基础设施安全保护、钓鱼邮件、数据安全、电信网络诈骗等常见网络安全防范事项分享了相关经验，团队的简端

良律师结合自身丰富的实务经验和多个刑事及行政处罚案例，对于网络安全不合规的各项行为尤其是帮信罪这一高发刑事犯罪作出了全面提示和解读，达到了良好的普法和宣传效果。

未来，泰和泰（武汉）律师事务所网络安全服务团队将继续加强与协会和各会员单位的联系，为维护网络安全贡献自己的专业力量。

首届武汉网络安全创新论坛收官，多项创新成果推进“中国网谷”建设

湖北日报讯（记者李源、杨然、通讯员黄立、蔡鑫伟）5 月 17 日，首届武汉网络安全创新论坛收官。在当天下午举办的主论坛上，从 31 项创新成果中脱颖而出的 10 项优秀成果正式发布。

此次论坛最大的亮点之一，是 5 月 16 日举办的数据安全、软件安全交流会。3 场交流会上，华为、中兴、奇安信、安天移动安全，以及中科院信息工程研究所、西安电子科技大学等国内网络安全、大数据行业龙头企业和高校、科研院所创新团队，携 31 项创新成果亮相。

“31 项创新成果涵盖隐私计算、政务云、机器学习、工业互联网等多个领域，代表业界领先水平。”软件安全创新成果交流会主持人、清华大学网络研究院教学

委员会主任段海新说，参会各方充分碰撞思想，不仅为企业优化提升已投向市场的创新成果指明方向，对创新团队提高研发质效也具有积极意义。

中科院信息工程研究所李凤华团队的“隐私计算理论和技术”此次获评优秀创新成果。李凤华介绍，2015年，中国学者在国际上率先提出并首次精准定义了隐私计算的概念和学术内涵。经过多年发展，隐私计算理论和技术不断成熟，可用于解决手机、平板电脑等智能终端频繁超范围采集个人信息，以及后台信息服务系统中隐私数据越权使用、大数据杀熟、个人画像结果被滥用、个人信息过度留存等问题，更好地保护用户数据安全。

除创新成果发布外，主论坛围绕筑牢网络安全屏障、强化数据管理工作等主题发布 4 份学术报告，发布《中国网络安全人才建设报告（2022 年）》《公众常用 App 个人信息保护指数报告》，签约启动网络安全学院学生创新资助计划二期项目，揭牌黄鹤网络安全实验室并启动黄鹤杯网络安全人才创新大赛。

武汉市相关负责人介绍，除主论坛外，本届论坛开展了 4 场创新成果交流会、6 场座谈会，设立了 1 场数字经济安全研讨会、1 场网安基地考察活动，1 场网安之夜活动。全面展示了我国网络安全人才培养、技术创新、产业发展前沿成果，专家学者共同探讨了网络安全基础性、战略性、前瞻性问题，创新打造了具有引领我国网络安全行业发展风向标作用的品牌大会。

来源：湖北日报

聚焦人才建设、个人信息保护，两份网络安全报告在汉发布

湖北日报讯（记者杨然、李源）5 月 17 日，在首届武汉网络安全创新论坛上，《中国网络安全人才建设报告（2022 年）》（以下简称《报告》）正式发布。《报告》首次针对网络安全领域人才培养供需两侧做出问卷调研，为网安人才的培养提供了基础数据和方向。

《报告》由中国网络空间安全协会联合行业专家共同编写，从中国网络安全人才发展总体现状、网安人才结构与分布，以及网安人才的培养和供需四方面做重点调研分析，深入探究了我国网安人才发展的现状及特点。

《报告》显示，目前国内网络安全领域人才队伍逐渐成形，人才培养机制渐趋成熟，人才供给不断增加，但依然存在高端专才紧缺、师资力量不足、人才供需不均衡等问题。

伴随着网民数量的不断提升，以及数字化、网络化、智能化的快速发展，各行各业对网络空间安全人才的需求愈发迫切。加强相关学科建设、人才培养，是如今推动网络空间安全事业发展的重要议题。《报告》提出，面向未来，网络安全人才建设应推动教育面向实践，强化网络安全教育学科体系建设，高度重视校企合作，不断提升能力、强化机制、优化模式、通畅供需，源源不断培养素质高、能力强、业务精的网安人才，为中国网安事业发展提供坚强保障。

当日，中国网络空间安全协会还发布了《公众常用 App 个人信息保护风险指数报告》。随着个人信息保护普法宣传教育不断深入，App 运营者已逐渐能够主动履行个人信息保护义务，一些互联网企业成立了专门的法务工作小组，深入研究 App 合规问题。同时，公众对个人信息的保护意识提高，对 App 违法违规收集和使用个人信息的投诉举报积极性也较高。多方共同努力，将推动数据安全和个人信息保护水平整体提升。

来源：湖北日报

推动智能汽车网络安全发展倡议书

智能汽车网络安全相关产业的企事业单位、高等院校和科研机构：

为深入学习习近平总书记关于网络强国的重要思想，贯彻落实市委市政府“要抢抓新能源汽车市场需求快速增长机遇，加快推动传统车企转型，积极引进新能源、智能网联汽车产业链企业在汉布局，推动我市汽车产业高质量发展”和“统筹发展和安全，高水平建设国家网安基地，加强关键核心技术攻关和网络安全人才培养，为筑牢国家网络安全屏障贡献武汉力量”的重要工作要求，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），向各单位倡议：

一、勇于责任担当，托起维护智能汽车网络安全重任

各单位应以高度的政治站位，增强责任感和使命感，承担起维护智能汽车产业网络安全的重任。不断提升车联网网络设施和网络系统安全防护能力、定期开展网络安全风险评估、加强网络安全值守、完善网络安全服务体系，做好车联网安全应急处置措施、构建网络安全信息共享机制，积极参加专委会或自行组织各项网络安全专业培训，通过系列措施为智能汽车产业发展和产品质量提升提供各层次网络安全保障。

二、加快科技创新，搭建产学研用交流合作共赢平台

各单位应加快科技创新和基础研究，充分利用好中国车谷产业基础和国家网络安全人才与创新基地资源优势。依托高等院校和科研机构与汽车和网络安全产业结合成紧密的优势学科，建立智能汽车与网络安全多学科融合、多团队协同、多技术集成的创新研发、技术转移、成果转化的合作平台，共同搭建政府监管、行业指导、企业参与、校企合作的智能汽车网络安全复合型人才培养平台。探索建立产业生态上下游对话协商与合作机制，共谋产业升级，共享创新成果。

三、加强行业自律，营造风清气正的行业发展环境

各单位应遵守并加强学习国家和行业相关法律法规，积极参与制定、推广和实践各项汽车网络安全标准和规范。加强自律监督和管理，促进汽车产业电动化、智能化、网联化过程中规范、健康、有序发展，抵制任何形式的不正当竞争，不制造不传播互联网有害信息，努力营造风清气正的行业发展环境和氛围，共同维护智能汽车行业参与者和消费者的网络信息安全合法权益。

我们怀揣着对智能汽车网络安全工作的热忱和责任，期待您的积极响应和支持。相信通过大家共同的努力，我们将会迎来一个更智能、更安全、更美好的出行未来。

武汉市网络安全协会

智能汽车网络安全专业委员会

2023年7月13日

我会指导的绿盟科技 2023 合作伙伴大会武汉站暨云化产品发布会成功举办

5 月 31 日，由武汉市网络安全协会指导，绿盟科技集团主办，汇志凌云、神州数码、中建材信息协办的“聚以致远 • 共筑新程——绿盟科技 2023 合作伙伴大会武汉站暨云化产品发布会”成功举办。百余位湖北区域的业界专家、合作伙伴齐聚江城，共同探讨数字化时代安全市场新机遇，分享云时代下的安全新技术。

武汉市网络安全协会秘书长刘悦恒为大会致辞。他表示，去年以来，协会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。绿盟科技作为副会长单位，长期为武汉市网络安全工作提供大量支持和帮助。2023 年 6 月 1 日是《网络安全法》正式实施六周年的日子。值此之际，组织召开“绿盟科技 2023 合作伙伴大会武汉站暨云化产品发布会”意义重大。希望各位嘉宾，能够通过协会与绿盟科技搭建的交流平台，充分互动，探索出网络安全新思路和新方法，共同为武汉网络安全事业贡献力量，持续扩大武汉网络安全品牌影响力。

绿盟科技集团产品行销部总监孟凡勇带来了题为《拥抱云端，独享百变能力——绿盟科技魔力防火墙 NF-SSE》主题分享，从“T-ONE CLOUD 的边界防护与响应思路”进行了深入剖析。在数字化转型推动下，企业网络呈现出边界模糊、大规模互联等特点，这种变化带来了安全互联、整网可视等新需求。基于弹性 + 运营的理念，绿盟科技推出了新一代边缘安全产品“魔力防火墙”。其以下一代防火墙为基础能力，通过云原生技术可弹性扩展全流量威胁检测、Web 应用安全防护等多维度安全能力，并可订阅运营服务，为用户打造弹性、可运营的一体化安全解决方案。

绿盟科技集团安全运营中心高级总监刘钟作《云时代下客户需要的安全》主题演讲。他提到，从某国际分析机构的报告可观察到，企业的信息建设已有全面云化的趋势，80% 的企业会选择混合云、多云架构来部署自己的业务，云化时代已全面到来。绿盟科技一直在技术变革中不断进行创新与突破，以客户为中心，构筑能够覆盖各类安全场景的全栈式云安全服务能力，赋能现代企业数字化发展，为客户提供更为全面、更加优质的数字化服务。

绿盟 T-ONE CLOUD 整合了绿盟科技最强的产品力和服务能力，创造性实现支持弹性异构的安全运营方案。绿盟科技集团云安全解决方案销售部总监薛竹君在演讲中提到，结合 T-ONE CLOUD 的四大核心组件——SOC 门户、魔力防火墙 NF-SSE、安全服务、手机 APP，把所有安全能力转化为服务通过云化方式交付到客户现场。T-ONE CLOUD 还可采用可信任的连接和访问机制，绿盟科技八大实验室研究实力赋能智慧安全大脑，保障高效检测，持续完善关键观测指标。

会议还特别邀请了武汉云视科技技术有限公司总经理李英作为合作伙伴代表登台分享。2021 年，武汉云视正式和绿盟科技签约，通过良好的项目合作，进一步加强了武汉云视与绿盟科技全面合作的信心。随着合作不断深入，武汉云视在 2022 年和 2023 年分别与湖北绿盟企业板块和科教文卫板块组成了虚拟团队，共同拓新、攻坚，也在不断寻求更全面的合作模式。她表示，绿盟科技作为安全行业先行者的优势很明显，希望未来和绿盟科技的合作更加深化，相互成就，走得更远。

云运营再造新安全。未来，绿盟科技将持续践行“智慧安全 3.0”这一兼具创新性与前瞻性的新一代网络安全创新理念，期待与客户和合作伙伴精诚合作，为更多用户提供“用得起，看得见，抓得全，管得住”的安全云服务，为用户数字化转型和业务创新保驾护航。


迎“六一”武网安协给孩子们带来了一堂生动的网络安全课

2023 年“六一”儿童节来临之际，为切实加强校园网络安全工作，增强中小学生网络安全意识，提高网络安全防护技能，自觉抵制网络不文明行为，净化校园环境，引导学生绿色上网，安全上网，谨防网络诈骗，近日，武汉市网络安全协会负责人受邀走进武昌未来实验小学美林校区开展“网络安全进校园主题活动。

协会秘书长刘悦恒通过视频课件、互动游戏、赠送网安宣传读本、问答等多种形式向同学们讲解了网络的优点和危害，共同学习网上自我保护方法，倡导践行《全国青少年网络文明公约》，一起学唱《网络安全拍手歌》。同学们在轻松快乐的氛围中认真学习，积极参与，充分认识到网络的优点和危害，学习了各种安全防范技巧。

网络的使用是一把双刃剑，安全上网是保证青少年健康成长的需要。此次活动使师生们对网络安全有了新的认识，增强了网络安全基本素质与防患能力，网络安全意识得到了明显提高。下一步，我会将继续加强网络安全知识的宣传和教育，帮助青少年正确使用网络，使网络成为他们的良师益友。

武汉市网络安全协会作为全市网络安全专业性社会团体单位，自协会成立以来组织了众多会员和专家开展网络安全下基层活动，走进企业走进校园，协会还积极协助主管部门推进中小学网络安全工作。

今年 2 月 28 日，武汉市网络安全协会发布了《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。本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。

武汉市网络安全协会会员互访交流活动第四期——走进武汉众邦银行

为了深入了解协会会员单位实际经营情况，相互学习各会员单位的先进管理经验和技术服务模式，围绕会员单位在网络安全事业发展中遇到的需求和问题，促进会员单位之间交流沟通与合作，提升协会服务能力，近日，以“凝心聚力共促发展，团结合作共保网安”为主题的武汉市网络安全协会第四期协会互访交流活动在武汉众邦银行股份有限公司（以下简称“众邦银行”）举行。

互访交流

武汉市网络安全协会会同部分会员单位代表一同走进众邦银行。专委会专家徐晟、奇安信、北信源、杭州安恒等协会成员单位相关负责人共同参与本次活动。协会轮值会长周佑源、秘书长刘悦恒、公共关系发展部主任严媛、数字资产保险网络安全工作部主任周韬、办公室主任张玉萍参加交流。

众邦银行金融科技管理部负责人田骏、安全管理团队经理张雯对协会领导、专家、各会员单位负责人的来访表示热烈欢迎，并带领一行人参观办公区域并讲解众邦银行的发展历程。

据了解，众邦银行由卓尔控股主发起，并联合其他多家湖北民营企业共同设立，是银保监会批准成立

的全国第 11 家民营银行，也是湖北省首家民营银行。众邦银行于 2017 年 5 月 18 日正式开业，初始注册资本 20 亿元，于 2020 年 1 月 16 日完成增资扩股，注册资本达到 40 亿元。

众邦银行定位于服务小微大众的互联网交易银行，于 2019 年获得国家高新技术企业认定，成立以来始终秉承“专注产业生态，帮扶小微企业、助力大众创业”的使命，以交易场景为依托，以线上业务为引领，以供应链金融为主体，以大数据风控为支撑，着力打造三个银行，即“打通交易与场景的互联网交易银行，致力于产融深度融合的供应链金融银行，数字化驱动科技赋能的开放型数字银行”。

截至 2022 年末，众邦银行总资产超 1000 亿元，客户总数超 4000 万户，共获得国家软件著作权授权 105 项、国家发明专利公开 133 项，综合实力稳居民营银行第一梯队。

在座谈交流环节，与会代表分别进行了自我介绍和发言，大家针对金融网络安全问题提出了很多建设性意见，并进行了深入沟通探讨。

武汉市网络安全协会专家委员会专家、中南财经政法大学金融科技研究院执行院长徐晟教授，围绕数智创新保障城市金融安全，结合武汉市数字经济发展趋势和众邦银行的“互联网”银行定位，与各位代表进行了深入交流。徐晟教授指出，通过公开信息了解到，武汉市委市政府正积极谋划推进政务信息数据、产业发展数据和金融业数据的共建共享工作，确保网络安全的前提下发展数字金融，使数智创新更好的服务于实体经济。众邦银行作为开放性的数字银行，率先在金融数字化转型中，带动湖北省与武汉市银行业上下游生态积极“走出去”，积极开展数字金融业务，实现数字金融创新，形成了较好的行业示范作用和影响力。当前高校人才培养工作也需进一步优化，传统金融人才培养工作应与时俱进，守正创新，希望金融行业与网络安全信息产业相互赋能深度融合，持续为金融科技进步提供智力和人才支持。

周会长、刘秘书长、徐教授代表武汉市网络安全协会为众邦银行颁发了协会会员单位牌匾和会员证书。刘秘书长表示，热烈欢迎众邦银行加入协会，并很高兴众邦银行成为我会第一家银行业团体会员。众邦银行的加入，既是协会网络安全工作深入金融行业服务科技金融的首次探索，也充分说明众邦银行高度重视网络安全工作，努力打造一家有着强烈安全基因的互联网银行。协会将竭诚为会员单位做好各项服务工作，在网络安全产业生态建设、产学研合作、人才培养等各方面，帮助会员单位排忧解难，与众邦银行一道加强网络安全与数智金融领域的合作，助力武汉网络安全产业健康快速发展。

武汉职业学院信创学院
邓小飞副院长来访我会

2023 年 6 月 5 日，武汉职业技术学院信创学院邓小飞副院长、教学秘书辜璇、学生科科长徐冰暘等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、政企服务部主任乔奇、公共关系发展部主任严媛、培训中心副主任向杰等热情接待，双方围绕着专业共建、社会培训及服务、毕业生就业事宜进行座谈交流。

座谈会上，邓小飞副院长介绍了武汉职业技术学院信创学院的创建的背景和目前发展的情况，还重点介绍武汉职业技术学院新创学院的师资、教学设施以及人才培养实践的模式。刘秘书长对邓院长一行表示热烈欢迎并介绍了协会的情况及近年来在主管部门的服务支撑，会员服务，实战化网络安全人才培养、团体标准的规划建设等重点工作。双方就后续在人才培养上依托教育技术及行业产业优势，在产学研用等各领域开展深入合作，产教融合协同育人。

会后我会积极协助信创学院 2023 届毕业生就业工作，深入了解会员单位用人需求，广泛发动组织会员单位参加信创学院 2023 届毕业生招聘会，武汉安域、吧嗒科技、华康科技等企业参与了本次招聘会，为毕业生提供就业机会及工作岗位。招聘会现场气氛热烈，同学们与企业招聘负责人积极沟通交流。各企业工作人员的专业解答，不仅让大家了解各企业人才需求和发展前景，同时也更加明确了自己未来的职业规划。

后续我会将持续对接高校及企业，紧扣企业人才需求，深化校企合作，为构建武汉超大城市网络安全防御体系提供持续的实战型人才供给。

武汉市网络安全协会走访武汉大数据公司

近日，武汉大数据产业发展有限公司正式申请并被批复成为我会会员单位（以下简称：武汉大数据公司）。6 月 16 日，武汉市网络安全协会轮值会长周佑源、秘书长刘悦恒等协会负责人一行专场走访武汉大数据产业发展有限公司并授牌。武汉大数据公司副总经理胡亚林、办公室综合总监杨琰等相关负责人热情接待并座谈交流。

据了解，2017 年，为抓住大数据产业发展的历史机遇，武汉市委市政府决策，成立武汉大数据产业发展有限公司。公司致力于构建以数据生态服务为核心的大数据产业，打造数字政府、培育数字经济、构建数字社会，践行数字中国战略。

协会负责人热烈欢迎武汉大数据公司加入协会，周会长表示，数据安全是国家安全的重要组成部分，数据泄露、丢失和滥用将直接威胁国家安全和社会稳定。近年来，国家高度重视、不断推进数据安全保护工作，数据安全领域法治建设不断完善。大数据公司的积极加入，充分说明了公司对安全工作的高度重视，也是我会深入数据安全工作搭建网络安全 + 数据安全专业化服务的新探索。刘秘书长介绍了协会近年来在主管部门服务支撑、会员服务、团体标准的规划与建设等重点工作，对武汉大数据在疫情期间利用数据赋能和技术支撑助力疫情防控的工作和在智慧城市、数字政府领域取得的成绩，以及对区块链产业的超前布局表示赞赏。

胡总带领协会参观了武汉大数据创新体验中心，详细讲解了公司在数据运营和政务服务方面的应用产品、专业服务能力和经营情况，并介绍了公司在政务服务和智慧城市方面的典型案例。

据了解，武汉大数据公司已经具备城市级数据归集治理及对外提供服务能力，先后承建武汉市数据共享交换平台和武汉市新型智慧城市数据归集服务等重点项目。公司自主研发的大数据能力平台，满足政府和企业打破“数据孤岛”、挖掘数据价值、释放数据效能的需求，并先后在各区、各地进行推广使用。

公司不断创新，在多年大数据应用项目基础上，形成了自主研发的大数据能力平台，为政府和行业用户提供一站式数据融合分析与系统功能服务，加速各类智慧应用场景落地，协助城市建设横向到边、纵向到底的“智慧城市”体系，为数字中国建设贡献智慧。

我会受邀出席 2023 年中国网络安全产业联盟会员大会并介绍武汉分站赛方案

6 月 20 日，2023 年中国网络安全产业联盟会员大会暨换届大会在北京隆重召开，我会应邀参会。

本次大会杨建军秘书长详细介绍了《2023 年中国网络安全市场与企业竞争力分析》报告的编制背景和研究思路，结合我国网络安全产业发展现状及最新动态，对 2022 年中国网络安全产业规模、市场格局与企业竞争力、产业发展趋势进行了全面分析，并公布了“2023 年中国网安产业竞争力 50 强、成长之星、潜力之星”（“CCIA50 强、成长之星、潜力之星”）榜单。

方华副秘书长介绍了“2023 年网络安全优秀创新成果大赛”相关情况及下一步计划安排。来自浙江省网络空间安全协会、四川省网络空间安全协会、武汉市网络安全协会、联盟数安委等大赛分站赛、专题赛的相关组织单位代表共同签署了自律承诺书。会议同时举办了“2023 年网络安全优秀创新成果大赛 - 安全严选专题赛”颁奖仪式，对安全严选专题赛评出的 40 项优

胜奖的获奖单位代表进行了颁奖，并为进入总决赛的 4 个项目颁发了总决赛通行证。

武汉市网络安全协会秘书长刘悦恒，代表武汉网络安全产业，向大会作《2023 网络安全优秀创新成果大赛—武汉分站赛介绍》报告。他用八组词，向与会嘉宾推介了自己的家乡武汉——大江大湖、九省通衢、科教之都、英雄之城、白云黄鹤、知音故里、光谷车都、网安基地。作为拥有全国网络安全人才与创新基地的国家中心城市，它还拥有着全国前三的科教资源、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。

本届 2023 年网络安全优秀创新成果大赛武汉分站赛，将在八月初在国家网络安全人才与创新基地迪马创聚场科技企业孵化器举办。本次大赛得到了武汉网络安全技术有限公司、武汉迪马创聚场科技孵化器有限公司、武汉安恒信息科技有限公司的大力支持。组委会将与“黄鹤杯”网络安全人才创新大赛创新成果擂台赛等省市网安大赛结合。按大赛规定，优秀产品与优秀解决方案排名前列选手不但可以拥有晋级全国总决赛等奖励，武汉分站赛还将单独设置奖项，提供丰厚奖品。

我会在中国网络安全产业联盟领导的见证下与浙江省网络空间安全协会、四川省网络空间安全协会负责人共同签署了大赛《自律承诺书》，本次大赛还将在杭州、成都同期举办分站赛。

武汉，已经在中国网安产业联盟的指导下连续成功举办了两届分站赛事。今年，协会将继续在各方的支持下，精心组织统筹安排，为选手和专家做好各方面支撑服务工作，为网络安全产业创新发展，打造舞台成就梦想，贡献武汉力量！

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

近日，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。

该专委会是华中地区首个在智能汽车网络安全领域的非营利性的专业性联合体。专委会的成立，是贯彻落实习近平总书记关于网络强国的重要思想，加快推进我市产业转型升级、构建现代化产业体系、推动经济高质量的发展的重要举措。专委会将致力于推动智能网联汽车的网络安全技术研发、检验检测等工作，加强智能网联汽车网络安全联动机制建设，为我市智能网联汽车产业高质量发展保驾护航。

随后，武汉市网络安全协会智能汽车网络安全专业委员会召开了第一次全体工作会议。会议由新当选专委会主任岚图汽车科技有限公司数智化部门负责人陶先锋主持，东风悦享科技有限公司、武汉路特斯汽车有限公司、武汉大学国家网络安全学院、华中科技大学网络空间安全学院、武汉理工大学计算机与人工智能学院、江汉大学人工智能学院 等 23 家委员单位参加会议。

本次会议审议通过了《武汉市网络安全协会智能汽车网络安全专业委员会 2023 年工作要点》和《推动智能汽车网络安全发展倡议书》。专委会成员单位共同呼吁：加强行业自律，营造风清气正的行业发展环境；勇于责任担当，托起维护智能汽车网络安全重任；团结合作共赢，共同搭建产学研用交流合作平台。

会议研究了《车联网网络安全检测技术要求》团体标准进展情况，专委会副主任委员单位湖北天融信公司作为标准发起单位，诚挚邀请专委会成员单位共同参与该标准的编写并提出相关工作建议。

附：专委会成员单位名单

（排名不分先后）

序号	单位名称
1	岚图汽车科技有限公司
2	东风悦享科技有限公司
3	武汉路特斯科技有限公司
4	武汉大学国家网络安全学院
5	华中科技大学网络空间安全学院
6	武汉理工大学计算机与人工智能学院
7	江汉大学人工智能学院
8	中汽研汽车检验中心(武汉) 有限公司
9	湖北省电子信息产品质量监督检验院
10	北京赛昇科技有限公司湖北分公司
11	武汉赛宝工业技术研究院有限公司
12	武汉安天信息技术有限责任公司

序号	单位名称
13	武汉安域信息安全技术有限公司
14	武汉安恒信息科技有限公司
15	曙光网络科技有限公司
16	湖北天融信网络安全技术有限公司
17	中国联合网络通信有限公司武汉市分公司
18	湖北珞格科技发展有限公司
19	开源网安物联网技术(武汉) 有限公司
20	武汉珈港科技有限公司
21	浙江远算科技有限公司
22	观源(上海) 科技有限公司
23	广电计量检测(武汉) 有限公司

武汉市网络安全协会第二届理事会第三次会议顺利召开

近日，武汉市网络安全协会第二届理事会第三次会议暨武汉市网络安全协会智能汽车网络安全专业委员会第一次全体工作会议在协会国家网安基地办公区顺利召开。

33 名协会理事单位和监事代表参加了本次会议。国家计算机网络应急技术处理协调中心湖北分中心、国家网络安全人才与创新基地办公室、武汉市委网信办网络安全处、武汉经开区工委网信办有关负责人到场指导。部分会员单位代表列席参加。

本次会议首先由第二届理事会第一期轮值会长武汉安域单位代表作任期工作总结。周佑源会长任期内带领协会出色完成了理事会交办的既定任务，扎实落实主管部门交办的各项工作，积极开展协会会员互访交流活动，高质量开展主题党日活动，持续推进协会团体标准工作，为武汉网安产业发展贡献了力量。

会议举行了协会轮值会长交接仪式，由第一期轮值会长单位武汉安域将轮值会长牌交接给第二期轮值会长单位湖北珞格。第二期轮值会长单位湖北珞格总经理管鹏飞向理事会作第二期轮值会长工作计划汇报。管会长表示，轮值期间协会将在网络安全宣传教育、会员信息分享与协作、网安调研与评估、加强生态建设、

加强协会会员服务等方面开展各项工作。

会议审议并表决了《武汉市网络安全协会团体标准经费管理办法》、《武汉市网络安全协会智能汽车网络安全专业委员会工作条例》、《武汉市网络安全协会智能汽车网络安全专业委员会负责人及委员提名名单》。

智能汽车网络安全专委会工作条例及人员提名名单议题审议通过后，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。专委会的成立，是协会深入学习习近平总书记关于网络强国的重要思想，深刻领会习近平总书记对网络安全和信息化工作作出的重要指示精神，贯彻落实市委市政府关于加快推进国家网安基地建设，做强网络安全等数字经济新业态，着力防范化解网信领域风险隐患，大力推动网信事业高质量发展，建设有全国影响力的科技创新中心的具体行

动，也是举旗帜聚民心、防风险保安全、强治理惠民生、增动能促发展、谋合作图共赢，勇担网络安全专业性社团使命责任的努力探索。

会议期间，三峡电子音像出版社常务副社长李翔作为特邀嘉宾向大家分享交流了网络安全科普读物编撰工作的经验和想法。

随后，协会及指导单位相关负责人向新入会会员：湖北航天信息技术有限公司、恒安嘉新（北京）科技股份公司、武汉易通科技有限公司、广电计量检测（武汉）有限公司、观源（上海）科技有限公司、上海竟安网络科技有限公司、泰和泰（武汉）律师事务所、国任财产保险股份有限公司湖北分公司等单位颁发会员证书及会员牌匾。

为发挥好政府管理部门与协会会员之间的桥梁和纽带作用，助力国家网安基地建设和发展，为网安基地各类入驻企业和专业人士提供政策辅导、资质申办、专业培训、标准制定、交流活动等协会服务，武汉市网络安全协会国家网安基地办公区正式揭牌并启用。

最后，各代表参观了位于协会办公区的迪马数智天地展厅。

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

2023 年 8 月 24-25 日，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。武汉分站赛由武汉市网络安全协会、武汉网络安全技术有限公司承办，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。

本次分站赛特别组织开展了参观交流活动，申报单位代表参观了国家网络安全人才与创新基地培训中心及黄鹤实验室，充分了解了国家网安基地发展环境和相关产业政策。

“2023 年网络安全优秀创新成果大赛”由分站赛、专题赛和总决赛组成，旨在推选我国网络安全产业优秀创新成果，搭建网络安全企业、技术、人才和资本合作平台，激发网络安全企业加强自主创新能力，推进网络安全产业结构化升级和高质量发展。分站赛在杭州、成都、武汉等三个城市举办，按照网络安全解决方案和创新产品分别评选出大赛优胜奖，并从优胜奖中推选优秀的项目入围总决赛。

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。

本次分站赛特别组织开展了参观交流活动，申报单位代表参观了国家网络安全人才与创新基地培训中心及黄鹤实验室，充分了解了国家网安基地发展环境和相关产业政策。

“2023 年网络安全优秀创新成果大赛”由分站赛、专题赛和总决赛组成，旨在推选我国网络安全产业优秀创新成果，搭建网络安全企业、技术、人才和资本合作平台，激发网络安全企业加强自主创新能力，推进网络安全产业结构化升级和高质量发展。分站赛在杭州、成都、武汉等三个城市举办，按照网络安全解决方案和创新产品分别评选出大赛优胜奖，并从优胜奖中推选优秀的项目入围总决赛。

我会支持并参与的武汉经开区举行智能汽车软件大会成功举办

9月5日，由武汉市网络安全协会支持并参与的武汉经开区举行智能汽车软件大会成功举办。武汉智能汽车软件园及智能汽车软件园发展有限公司成立，武汉智能汽车软件园建设三年行动方案发布，为经开区打造智能汽车软件和车规级芯片产业高地，建成全国领先的智能汽车软件创新中心，加快武汉建设中国软件特色名城提供有力支撑。

中国工程院外籍院士、清华大学智能产业研究院院长张亚勤，中国卫星导航定位协会会长于贤成，中国软件行业协会副秘书长杨菊，武汉大学党委常委、副校长唐其柱，武汉理工大学党委副书记孟芳兵，国家知识产权局专利局专利审查协作湖北中心党委书记侯海薏，省经信厅党组成员、总工程师盛章学，市委常委、武汉经开区工委书记刘子清，江汉大学党委书记覃道明，武汉商学院党委书记刘志辉，武汉经开区工委副书记、管委会主任唐超出席活动。

东软集团创始人、董事长刘积仁，科大讯飞总裁吴晓如，中国信科原党委书记、董事长童国华，湖北移动董事、副总经理韩晓雷，以及来自全国的智能汽车软件及相关行业企业家出席活动。

盛章学在致辞中表示，未来，汽车智能化将成为各大车厂竞逐的焦点，不断提升软件能力将成为定义整车功能的关键，成为湖北汽车转换赛道的关键。武汉经开区是全省汽车产业的主引擎，发展智能网联汽

车可为恰逢其时、恰逢其势、大有可为，希望经开区抢抓机遇，围绕产业链布局创新链，围绕创新链布局产业链，构建智能网联汽车新生态，推动湖北智能网联汽车产业创新发展，为建设全国构建新发展格局先行区贡献更大力量。

杨菊表示，智能汽车的灵魂是软件，智能汽车软件的发展水平已经成为衡量汽车价值的重要标准，软件和服务能力成为未来汽车产业最重要的竞争力。希望今天在场的行业专家和软件企业围绕“软件定义汽车，智能引领未来”各抒己见，深入开展思想交流，达成合作共识，为武汉智能汽车软件发展建言献策，为我国汽车软件自立自强贡献更多力量。

唐超向企业家、行业精英发出邀请，他表示，为抢抓“软件定义汽车”新赛道，武汉经开区在毗邻南太子湖区域，规划 1 平方公里的武汉智能汽车软件园，并将配套发布“软件十条”扶持政策，打造“软件定义汽车”创新策源地。经开区诚挚邀请各位企业家来这里投资兴业，共同建设车谷产业创新大走廊。

当天，张亚勤、于贤成、童国华、刘子清共同为武汉智能汽车软件园揭牌。

刘积仁、吴晓如、韩晓雷、唐超共同为武汉智能汽车软件园发展有限公司揭牌。

张亚勤、童国华、刘积仁、吴晓如获聘武汉智能汽车软件产业发展顾问，将为武汉经开区智能汽车软件产业发展提供高水平的决策建议和智力支持。

作为首批入驻软件园的企业之一，东软南方研发基地将于明年一季度交付投入运营，“南方研发基地的定位是为汽车提供完整软件解决方案，人员规模预计达到 4000 人。”刘积仁说。

今天，科大讯飞星火认知大模型正式向社会发布，“未来，在武汉智能汽车软件园中，科大讯飞会专门提供面向汽车的通用认知技术平台，使通用人工智能的各种应用功能在经开区的场景应用里率先推出来，形成示范性的应用。”吴晓如介绍。

现场，湖北省车联网安全产业技术创新研究院、吉利汽车研究院武汉研发中心、中科微电子研发中心、法雷奥舒适与辅助驾驶研发中心等 10 个智能汽车软硬件领域重大项目签约，项目涵盖了智能网联汽车、车联网、智能座舱、高端核心芯片等产业，将进一步发挥智能汽车软件和车规级芯片在智能网联和新能源汽车领域的赋能、赋值、赋智作用。

此外，武汉经开区分别与中国软件行业协会、湖北省软件企业协会、武汉市软件协会签订武汉智能汽车产业园战略合作协议，与中国银行、湖北银行、工商银行等多家金融机构签订武汉智能汽车软件园金融共建协议，共同推动软件产业高质量发展。

刘积仁、吴晓如等企业大咖在现场分享行业发展最新前沿动向，共话推动软件产业高质量发展。

武汉市相关部门负责人，华中科技大学等院校领导、武汉市网络安全协会及兄弟行业协会负责人，金融投资机构、银行代表，武汉经开区有关领导参加活动。

出品：武汉经开区工委宣传部
武汉经开区融媒体中心
采写：记者张隽 摄影李岿
通讯员李建沂 杨柳 陈安俊
编辑：吕作璐 蒋秋雨
注：此文转载时略有修改
图片来源：市网安协会、荆楚网

我会智能汽车专委会成员单位签约共建智能网联汽车信息安全检测中心

10 月 17 日，武汉市网络安全协会智能汽车网络安全专业委员会两家成员单位——开源网安与湖北省电子信息产品质量监督检验院签署战略协议，并举行了“智能网联汽车网络安全检测中心”揭牌仪式。该检测中心的成立，是充分贯彻落实习近平总书记关于网络强国的重要思想，也是智能汽车网络安全专委会致力于加快推动我市产业升级转型、培养高素质人才、推动经济高质量发展的重要举措，为智能网联汽车网络安全保驾护航的具体行动，推动成员单位合力打造全国首家质检口领域的网联汽车网络安全检测中心。

湖北省经济和信息化厅人工智能和大数据产业处、湖北省电子信息产品质量监督检验院、武汉市产业创新发展研究院，东风岚图汽车，湖北大学，武汉软件工程职业学院、开源网安公司等相关负责人出席本次活动。我会秘书长刘悦恒，办公室主任张玉萍，智能汽车网络安全专业委员会秘书长郝晓峰受邀出席并见证本次签约及揭牌。

武网安协两项团体标准正式启动

近日，武汉市网络安全协会（以下简称武网安协）两项团体标准启动会在烽火创新谷正式召开。本次启动的两项团体标准《制造业数据安全管理中的数据分类分级方法指南》和《智慧园区网络安全防御体系建设指南》由智网安云（武汉）信息技术有限公司（以下简称智网安云）提出并牵头编制。武网安协相关负责人，智网安云总经理周阳波、副总经理梁忠辉分别代表标准发布单位和牵头单位出席本次会议，华中师范大学、湖北大学、中国电信股份有限公司武汉分公司等12家单位代表参加了本次活动。

启动会上，由武网安协政企服务部主任乔奇宣贯了《团体标准管理办法》；智网安云团标起草组相关负责人介绍了两项标准的框架及实施计划；参编单位与会代表就标准框架和实施计划进行了充分讨论，并提出了建设性的意见和建议。标准起草组将汇总整理相关建议，进一步修改和完善标准内容。

根据《国家标准化法》、《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，结合会议讨论意见和建议，牵头单位智网安云发布了标准制修订工作初步计划，本月开始两项团体标准编制工作组将分步启动开展标准起草、编写工作。

参编单位代表一致认为，通过本次深入研讨和交流，明确了两项团体标准的编制思路、各方职责和分工，为进一步推进两项团体标准更加科学、合理、规范地开展编制工作，奠定了基础。

武汉市网络安全协会将继续携手理事单位智网安云等头部企业，通过搭建数据安全管理标准化交流平台，邀请行业内各领域专家学者和单位代表深入交流合作，通过持续推进各项标准化工作，促进我市网络安全和数据安全工作的健康快速发展。

“首席安全官 (CSO) 能力水平评价标准”第一次筹备工作会议顺利召开

2023 年 10 月 24 日，由武汉市工业信息化中心和武汉企业信息化促进会、武汉市网络安全协会共同牵头的《首席安全官 (CSO) 能力水平评价标准》（以下简称标准）第一次筹备工作会议顺利召开。长飞光纤、华工正源、安恒信息、星野科技、网御星云、乾越信息等相关单位专家代表出席会议。会议由中心副总工胡颸主持。

会上，胡颸副总工对各参编单位的参与和支持表示感谢，对此标准编制的紧迫性和必要性进行说明，并对编制工作提出希冀与要求。主编单位代表乾跃信息总经理上官含章介绍了标准编制背景、编制原则和主要内容。与会专家就标准的适用对象、评价方法、框架结构和各章节重点内容等方面内容进行了深入的讨论和交流，提出了许多建设性的建议和意见。

下一步，编制小组将根据此次会议各位专家的意见与建议，把好本标准的定位和方向，尽快修改完善标准草案。希望全过程都得到行业企业和专家的大力支持，推动标准编制阶段成果先行先试，不断论证和优化，加强调研和研讨，提升标准适应性和可操作性，为企业的信息安全岗位提供评价标准，进一步提升企业信息网络安全整体水平。

武网安协轮值会长工作交接顺利完成

2023 年 11 月 10 日，武汉市网络安全协会在武汉东湖科技保险发展促进中心举行了第三期轮值会长工作交接仪式。根据《武汉市网络安全协会轮值会长工作制度》相关规定，第二届理事会第二期轮值会长湖北珞格科技发展有限公司（以下简称湖北珞格）总经理管鹏飞作轮值任期工作总结。

管鹏飞会长表示，任期内通过与协会各成员单位和秘书处同事通力配合，出色完成了既定任务，扎实落实主管部门交办的各项工作，举办了形式多样的网络安全宣讲、创新性标准研讨和线下各类活动，吸引了众多会员的积极参与。通过这些活动，不仅增进了会员之间的交流与合作，还提升了协会在网络安全领域的知名度和影响力。最后，管会长向与会代表表达了对协会成员的感谢和祝福。他回顾了自己担任会长期间取得的成绩和经验，并希望新一届轮值领导能够继续推动协会各项事业的持续发展。

本期轮值会长交接仪式上，第二期轮值会长管鹏飞向第三期轮值会长——湖北天融信网络安全技术有限公司政府事业部总经理吕露正式交接。随后，吕会长向与会代表表示感谢，她承诺将继续加强协会内外部资源的整合，促进协会在网络安全领域的影响力和地位。

她表示，在轮值期间将继续与协会同仁卓厉奋发，共同努力：一、加强网络安全的普及与教育。利用多媒体平台，持续开展网络安全知识宣传活动，提高公众对网络安全的重视。二、深化会员间信息互通与资源共享。构建会员之间的信息交流平台，实时更新网络安全动态，分享最新的安全研究和情报。三、强化网络安全分工合作机制。建立虚

拟网络安全协同保障团队。加强与政府、学术机构、企业联手，共同推进网络安全技术的研发与应用。四、策划并组会员大会，总结工作成就，展望未来发展趋势，强化会员的凝聚力和身份认同感，促进知识和信息的分享，同时，根据会员的反馈和建议调整和优化未来的工作计划，确保协会的工作始终贴合会员需求，推动行业的持续健康发展。

随后，两任轮值会长共同向新入会的成员单位：中国平安财产保险股份有限公司颁发会员标牌和证书；向新晋升的理事单位：湖北天地和兴科技有限公司颁发理事标牌和证书。

武汉市网络安全协会轮值会长制度是为进一步促进协会日常工作的开展，充分发挥协会会长、副会长以及理事的职务作用，调动广大会员的积极性和团队协作精神制定的一项工作举措。本次工作交接仪式将为协会进一步发展注入新的活力和动力。相信在新任轮值会长的代领下，协会将进一步壮大，并为武汉市乃至全国的网络安全事业做出更大贡献。

我会《数字资产网络安全风险量化评估规范》团体标准编制工作正式启动

2023 年 11 月 9 日，由武汉市网络安全协会主办、武汉东湖科技保险发展促进中心支持并承办的《数字资产网络安全风险量化评估规范》团体标准启动会在光谷科技大厦召开。

本次启动的《数字资产网络安全风险量化评估规范》团体标准由武汉华康科技有限公司提出，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华康公司总经理周韬主持。

武汉东湖科技保险发展促进中心主任孙智在致辞中表示，科技保险需要服务数字经济时代的需要，网络安全保险是保险业面临的新的服务领域，市场有迫切的需求，发展有广阔的空间，对网络风险科学地进行识别、评估和量化，是开展网络安全保险的前提条件，解决网络风险量化评估，将对我们开展网络安全保险产生积极的作用。希望各位专家以创新的精神、过硬的技术、务实的作风做好课题研究，争取撰写出全国一流的、对网络安全风险管理产生积极作用的成果。

武汉市网络安全协会秘书长刘悦恒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、范围和预期效果、文本结构、工作计划与分工等标准编制具体工作。中南财经政法大学金融学院徐晟教授、湖北经济学院金融学院刘畅教授、湖北省电子信息产品质量监督检验院软件测评中心主任李新、国任财产保险股份有限公司湖北分公司副总经理吴涛、湖北天融信网络安全技术有限公司政府事业部总经理吕露、上海竟安网络科技有限公司总经理吉贻俊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。

武汉大学、中南财经政法大学、江汉大学、湖北经济学院、汉口学院、武汉东湖科技保险发展促进中心 、中国平安财产保险股份有限公司、国任财产保险股份有限公司、武汉路特斯科技有限公司、上海竟安网络科技有限公司、湖北公众信息产业有限责任公司、北京长亭科技有限公司、湖北天融信网络安全技术有限公司、深圳市科力锐科技有限公司、湖北省电子信息产品质量监督检验院、武汉明嘉信技术有限公司、湖北连邦云创科技有限公司、湖北珞格科技发展有限公司、武汉安经纬业信息安全技术有限公司等约二十家单位 40 多位代表参加了本次团体标准编制启动会。

武汉市网络安全协会将继续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和专家参与，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。

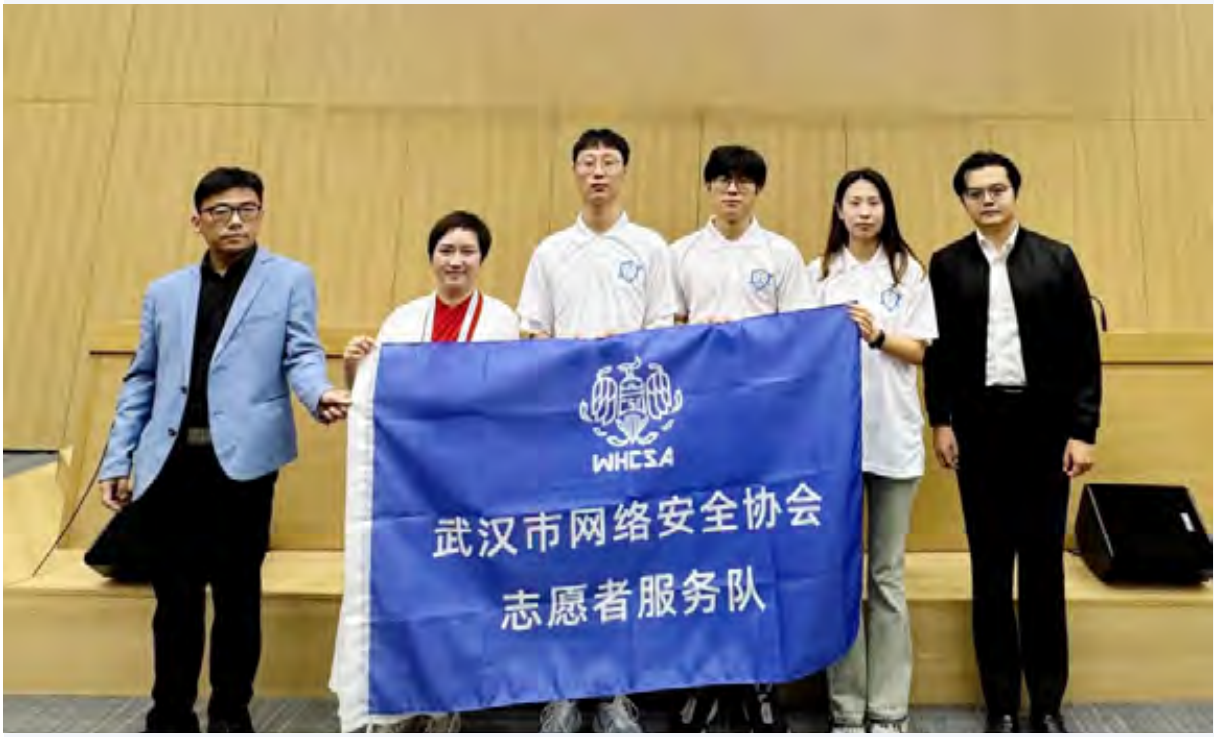
背景介绍

今年 7 月，工业和信息化部 国家金融监督管理总局今年联合发布了《关于促进网络安全保险规范健康发展的意见》文中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。开展网络安全风险量化评估，探索建立网络安全风险量化评估模型，加强网络安全风险影响规模预测、经济损失等分析。支持网络安全企业、专业网络安全测评机构等研发网络安全风险量化评估技术，开发轻量化网络安全风险量化评估工具，鼓励保险机构建立网络安全风险理赔数据库，支撑网络安全风险精准定价。

武汉目前拥有中央网信办授予的全国首个“国家网络安全人才与创新基地”和中国银保监会与湖北省政府批准设立的全国首个“国家级科技保险创新示范区”。今年春，武汉东湖科技保险发展促进中心和武汉市网络安全协会正式签订战略合作协议，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。今年 7 月，网络安全保险成为武汉东湖高新区科技保险险种拟试点并给予补贴。

综上，对于从事网络安全和科技保险的从业者和机构而言，在武汉从事网络安全保险和网络安全风险量化工作，可以借助武汉独特的“网络安全 + 科技保险”双料国家级平台资源优势和交通区位与科教优势，主动创新、加强合作、赋能产业，获得更多更全的场景应用并向全国进行推广，从而发挥更大的示范价值。

武汉市网络安全协会志愿者服务队正式成立



近日，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。

网络安全建设是国家安全建设的重要环节，成立网络安全志愿服务队意义重大，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，营造和维护优良的网络环境需要全社会的广泛参与和各方的共同努力，共同推动网络安全建设事业的良性发展。

武汉市网络安全协会志愿者服务队成立后将在主管部门的指导下，用实际行动践行奉献、友爱、互助、进步的志愿精神，不断挖掘培养网络安全专业人才，充分发挥当代网络安全青年志愿服务力量，助力大武汉建设，打造召之即来、来之能战、战之必胜的网络安全志愿者队伍。

下一步，武汉市网络安全协会将进一步完善志愿者队伍的管理工作，扩大志愿者队伍规模，建立长效培训机制，加强网络安全人才培养，为筑牢国家网络安全屏障贡献武汉力量。

《车联网网络安全检测技术要求》团体标准编制工作正式启动

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。智能网联汽车是搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与车、路、人、云端等智能信息交换、共享，具备复杂环境感知、智能决策、协同控制等功能，可实现“安全、高效、舒适、节能”行驶的新一代汽车。在产业快速发展的同时，车联网安全风险日益凸显，车联网安全保障体系亟须健全完善。

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，推动产业链创新链深度融合，协助主管部门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，促进汽车数据合理开发利用，由武汉市网络安全协会批准立项并归口、湖北天融信网络安全技术有限公司牵头的《车联网网络安全检测技术要求》团体标准启动会顺利召开，会议通过线上形式进行。

武汉市公安局交通管理局、武汉大学、华中科技大学、武汉理工大学、湖北大学、东风汽车集团技术中心、岚图汽车科技有限公司、东风商用车有限公司、武汉达安科技有限公司、东风汽车集团股份有限公司猛士汽车科技公司、湖北省电子信息产品质量监督检验院、武汉赛宝工业技术研究院有限公司、武汉安域信息安全技术有限公司、开源网安物联网技术（武汉）有限公司、湖北邮电规划设计院、宝牧科技（天津）有限公司等有关专家和代表参加了本次会议。

武汉市网络安全协会相关负责人首先介绍了协会团体标准有关情况，智能汽车网络安全专委会负责人介绍了专委会前期工作情况，天融信技术专家孙亚飞对本项团体标准的立项背景、标准框架和有关国家标准的衔接做了说明。各位专家针对选题方向、标准文本结构和车联网安全检测的技术路径等专业问题进行了深入探讨。

天融信公司吕露代表标准起草单位表示，本次立项的团体标准起草单位涵盖了交通主管部门、高校、车企、检验检测机构和网安头部企业，比较完整的代表了智能网联汽车各相关方，本项标准要进行深入调研听取各方意见，力争作为国家标准与行业标准的聚焦版、增强版和升级版，满足我国智能网联汽车网络安全检验检测实际需求，希望各参编单位和专家充分发挥各领域专长，加强合作交流，高质量高水平完成本次起草编制任务。

全国基础软件安全可信行业产教融合共同体在汉成立

12 月 15 日，全国基础软件安全可信行业产教融合共同体成立大会在武汉隆重召开。武汉市网络安全协会作为受邀嘉宾参加了成立大会。大会公布了共同体成员单位名单，我会成功当选常务副理事长单位。

全国基础软件安全可信行业产教融合共同体由统信软件技术有限公司、武汉大学、武汉职业技术学院牵头，联合相关企业、行业协会、有关院校、科研院所等 100 多家单位自愿组成职业教育联合体与利益共同体，将以人才培养为核心，以产教深度融合为手段，推动全国基础软件安全可信行业的发展。

全国基础软件安全可信行业产教融合共同体将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，以立德树人为根本，以“产教融合、职普融通、科教融汇”为主线，坚持平等互利、诚信合作、务实创新、多元共原原则，汇聚政行企校各方资源，以教促产、以产助教、产教融合、产学合作，延伸教育链、服务产业链、支撑供应链、打造人才链、提升价值链，推动形成同市场需求相适应、同产业结构相匹配的现代职业教育发展新格局，培养高素质复合型技术技能创新人才、能工巧匠、大国工匠，助力数字中国、教育强国、科技强国、人才强国建设，为中国式现代化强国建设贡献力量。

2023 年湖北省国家基地“楚慧杯”网络空间安全实践能力竞赛决赛圆满落幕

12 月 23 日，由省委网信办、省教育厅指导，武汉市委网信办、武汉市教育局联合主办，武汉市互联网行业联合会承办，武汉市网络安全协会等协办的 2023 年湖北省“楚慧杯”网络空间安全实践能力竞赛，在国家网安基地进行决赛争夺和闭幕颁奖。

本次竞赛以科学合理的赛程设置、强调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。预赛采用主流 CTF 夺旗赛模式。通过竞赛平台提供 WEB、CRYPTO、PWN、REVERSE、MISC 等类型的赛题，设置动态积分制，考验选手的解题速度和策略调整能力。决赛把新颖的 AWDP（Break+Fix）攻防赛融入竞技环节，使得竞赛更具全面性和挑战性。

湖北省“楚慧杯”网络空间安全实践能力竞赛至今已成功举办七届，累计近 3500 支战队同台竞技、反响热烈。本届竞赛移师国家首个网安基地，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，为大家奉献了一场白”与“黑”的巅峰对决，“红”与“蓝”的极限对抗，展现了网安人护网安民的独门绝技和不断挑战自我的青春风貌！

“楚慧杯”已经成为湖北网络安全事业一张亮丽的名片，借助赛事的举办，不断发掘网安新星，持续传递友谊火种，共同推进国家网安基地建设，为湖北武汉塑造发展新动能新优势、推动高质量发展提供有力支撑。

获奖名单

一等奖：天权信安

二等奖：n1udotbanm4n、肆方安全实验室、NEURON

三等奖：SDC_DMW、星相实验室玉衡战队、n、Kap0k、火锅不加辣

优胜奖：L3h_ForeverOld、Xp0int、汪汪队爱吃鸡公煲、瑶光战队、FHT、noname、北极星

我会与全国互联网安全行业产教融合共同体正式签订合作协议

近日，互联网安全行业产教融合共同体成立大会在武汉召开。湖北省委网信办、湖北省教育厅、武汉市委网信办、武汉临空港经济开发区、中国教育发展战略学会产教融合专业委员会、以及首批 102 所院校、33 家企业的领导，出席了共同体成立大会及揭牌仪式。

互联网安全行业产教融合共同体（以下简称“共同体”）是由湖北省委网信办、湖北省教育厅、中国教育发展战略学会产教融合专业委员会指导，北京天融信网络安全技术有限公司、华中科技大学、湖北生物科技职业学院牵头发起，联合国内普通高校、职业院校、科研机构、上下游企业，行业组织等共同参与的全国性、行业性产教融合组织。

会议同期，天融信科技集团、华中科技大学、湖北生物科技职院、武汉市网络安全协会四家单位举行了“网络安全行业产教融合签约仪式”。未来，共同体将以发展建设教学资源库、产业入校、实战人才提升等方面作为重点，着力推进与行业企业、院校、科研院所的多元合作，并结合武汉网络安全产业特色，形成紧密合作，推动校企与地方产业的深度融合，共同为国家网络安全人才与创新工作，贡献力量！

武汉市网络安全协会 2023 年第二批新增会员介绍

1、湖北航天信息技术有限公司

湖北航天信息技术有限公司是中国航天科工集团有限公司下属航天信息股份有限公司（股票代码：600271）在湖北地区设立的以信息安全为核心技术的高新技术企业，于 2002 年 4 月 12 日成立，注册资本 3350 万元。公司依托航天的技术优势、人才优势和组织大型工程的丰富经验，面向政府（行业）、企业信息化市场，提供信息技术服务和一体化解决方案，在智慧税务、电子票据、企业财税服务、金融科技服务、公安、智慧政务、教育、网络安全等领域服务政府和企业客户。

为了落实科工集团与航天信息十四五发展规划，推动科工集团在鄂实体企业高质量发展，加快在信息安全领域的产业布局。同时，基于国家对于网络强国建设高度重视，公司与公安部第三研究所、武汉市经开区合作建立楚天数字经济网络安全产业园，引入网络安全等级保护和安全保卫技术国家工程研究中心数字经济网络安全分中心、城市网络安全与网络事件防控技术服务中心、院士创新中心—标准研究和验证中心、数字经济安全能力验证基地、数字经济安全人才教育培训基地与数字经济网络安全宣传交流基地，构建城市网络安全基础设施和网络安全综合防御体系。

2、恒安嘉新（北京）科技股份公司

恒安嘉新是提供“云 - 网 - 边 - 端 - 用”综合解决方案的大数据智能运营运维产品，服务于产业互联网的科技工程企业。创立十余年来，始终专注于通信网和互联网数据智能分析领域，赋能智慧治理、智慧网络、智慧警务、智慧工业、智慧农业、智慧金融、智慧医疗、智慧教育等场景，为政企客户提供新一代网络信息安全、数据分析、智能业务应用解决方案和“管家式”运营运维服务。

公司围绕“专、精、特、新”理念，打造了覆盖采集、分析、认知、决策的全链条智能体系；拥有通信网和互联网海量数据实时处理技术、具有深度学习能力的智能安全引擎技术、“云—网—边—端—用”综合治理技术、大数据知识中台等核心技术、安全研运一体的服务体系；研发了网络空间安全综合治理、企业安全、5G 通信网数据智能应用产品和运营运维服务，具备“云→端”准确识别、“云→网”快速联动、“云→边”智能分析、“网→端”精准处置、“端→用”协同运营能力。

公司产品遍布全国 31 个省，支撑工信等网络安全主管部门、电信运营商在骨干网、城域网、移动互联网、工业物联网、企业网的数千个节点部署了 NTA“网络摄像头”，提供全天候、全方位的大数据智能分析产品和服务。

公司现有员工上千人，汇聚了通信、安全、AI 等领域的优秀人才；公司是连续 10 多年的国家级网络安全应急服务支撑单位；设有博士后工作站和云网创新研究院；参与制定上百项国家和行业标准；获得数十项发明专利和软件著作权；多次夺得人工智能、工业互联网、网络攻防竞赛桂冠；为“建党 100 周年”、“国庆 70 周年”、“十九大”、“两会”等国家级重大活动提供安全保障；成功入围国家级专精特新“小巨人”企业；第五空间反诈平台避免和挽回群众损失数亿元。

3、武汉易通科技有限公司

武汉易通科技有限公司成立于 2003 年，注册资金 5118 万元人民币，位于洪山区融创智谷，是智慧解决方案提供商、系统集成业务服务商。公司致力于提供系统集成、智慧政务、智慧城市、信息服务、自主可控解决方案及实施，为政府和企业客户提供完善、创新、一流的服务。目前公司已有涉密信息系统集成甲级资质、电子与智能化专业承包二级资质、安防工程

企业设计施工维护能力二级资质、信息技术服务运行维护标准（二级）符合性认证、计算机信息系统集成三级企业资质、高新技术企业认定、软件企业认定证书、CMMI5 软件成熟度认证、AAA 资信认定证书、ISO9001 质量管理体系认证、ISO20000 IT 服务管理体系认证、ISO27001 信息安全管理体系认证证书、ISO14001 环境管理体系认证、ISO45001 职业健康管理体系认证等相关资质。

武汉易通科技有限公司经过数年的经营与积累，凝聚了一批高素质的科研技术和管理人才，发展成为一家中型规模的高科技企业。公司业务范围覆盖全省，2013 年公司设立襄阳分公司、恩施办事处。公司成立以来，始终以客户需求为导向，在政府、军工、医疗、教育、金融、能源等多个行业积累了众多的成功案例与实施经验，获得了良好的口碑和赞誉。

4、广电计量检测（武汉）有限公司

广电计量检测 (武汉) 有限公司成立于 2014 年 03 月 25 日，注册地位于洪山区鲁磨路 488 号（第六九 0 七工厂内），广电计量检测（武汉）有限公司是广州广电计量检测股份有限公司根据行业发展趋势和战略规划，为更好地服务华中地区客户在湖北省武汉市投资设立的全资子公司。具备军工、通信、医药、食品、汽车、电子、第三方检测机构、企事业研究所、医院、电力等行业的仪器设备参数齐全的计量校准能力，能力覆盖行业面较广，客户覆盖几乎湖北省各行工业企业的标杆企业。

5、观源（上海）科技有限公司

观源（上海）科技有限公司始于 2014 年，公司总部位于上海市闵行区紫星路 588 号 2 号楼 5A-01 室，是以密码技术为核心的信息安全产品及解决方案提供商。公司聚焦商用密码、隐私计算、区块链等技术在芯片安全、移动安全、数据安全、关键信息基础设施保护等方面的创新应用，致力于以“密码创新，推动安全数字未来”。

6、上海竟安网络科技有限公司

竟安科技是国内首家专注于企业级网络安全风险量化评级的创新高新企业，成立时间 2017 年，总部位于上海，企业主创团队均来自国内头部互联网企业安全核心团队，以安全大数据和威胁情报为基础，自主研发了基于风险大数据的企业安全评级系统（瞭望塔），解答用户核心痛点。帮助企业自动化识别、量化并降低企业网络安全风险的同时，提供持续监控、执行报告，网络保险，供应链可见性，财务量化等能力。

7、泰和泰（武汉）律师事务所

泰和泰律师事务所是一家人数规模位居中国律师行业第一阵列，且已荣晋全球律所规模百强的覆盖中国连接世界的大型综合性律师事务所。成立于 2000 年 5 月，历经 20 余年持续高速发展，已在北京、成都、重庆、贵阳、济南、昆明、拉萨、深圳、上海 . 天津、香港、西安、太原、西宁、南京、武汉、海口、乌鲁木齐、福州、广州、南昌、郑州、华盛顿、悉尼、加德满都

及曼谷等国内外主要城市设立了办公机构，各办公室实力均居于本地前列。

泰和泰武汉办公室于 2020 年 4 月 29 日设立，是泰和泰在长流域的又一重要布局，为泰和泰进一步加强与长江经济带的法律服务联动提供强大动力。

泰和泰武汉办公室现已吸引了诸多业内有专业优势的领军人才和专业人才，并汇集了一批专家顾问。合伙人和律师大多来自武汉大学、中南财经政法大学、华中科技大学、武汉理工大学、华中师范大学等知名院校，拥有多位博士，并在省、市律协担任重要职务。本所合伙人、律师具有丰富的实务经验和深厚的理论功底，并已形成多个具有核心竞争力、创新发展的专业化部门。

8、国任财产保险股份有限公司湖北分公司

国任财产保险股份有限公司（简称“国任保险”）是经国务院金融监督管理部门批准，于 2009 年 8 月成立的一家全国性保险公司。目前，公司注册资本 40.07 亿元，注册地为深圳，设有二级机构 26 家，三级及四级机构 200 余家，机构网点已基本覆盖全国重点经济区域。

国任保险具有深厚国资背景和股东优势，第一大股东为连续三年入选《财富》世界 500 强的深圳市投资控股有限公司，持股比例 41%；其他股东包括联美量子、罗湖投控、中国信达、中国铁建等 18 家大中型央企、地方国企和优秀民营企业。

作为深圳市属国资控制的唯一财险公司，国任保险拥有一支高素质、专业化的管理团队，管理团队核心人物拥有中央部委、行业监管、保险主体等多元背景，熟悉宏观经济和保险发展规律，视野开阔、能力突出、素质全面，带领国任保险不断开创事业发展新局面。

国任保险既有国有企业的体制优势，也有市场化的机制优势。2019 年以来，在新领导班子带领下，国任保险全面推进深化改革、创新转型、价值发展，经营业绩逆势而上、跨越发展。2021 年，正式迈入财险主体“百亿俱乐部”。2022 年，排名财险市场第 14 位，实现四年连续盈利。截至目前，累计为 3200 余万个人、企业、政府等客户提供服务，提供风险保障超过 43 万亿元，累计赔付近 300 亿元。

9、中国平安财产保险股份有限公司湖北分公司

中国平安财产保险股份有限公司湖北分公司于 1995 年成立，是中国平安财产保险股份有限公司在湖北省设立的全资省级分公司。经过近 29 年的发展，截至目前，平安产险湖北分公司下设 15 家三级机构、121 家四五级机构，共有正式员工 2781 人，覆盖全省所有县域网点。

平安产险湖北分公司经营业务范围涵盖企业财产损失保险、家庭财产损失保险、短期健康保险、意外伤害保险、建筑工程保险、安装工程保险、货物运输保险、机动车辆保险、船舶保险、能源保险、法定责任保险、一般责任保险、保证保险、信用保险、种植保险、养殖保险等一切法定产险业务及国际再保险业务。

近年来，公司承保了多项国家重点工程及省内外工程项目，依托平安集团综合金融和科技优势，始终坚持“保险为民”的本色，发挥专业能力，持续创新产品和服务，满足人民对美好生活的追求，让客户“省心、省时、省钱”。在“专业，让生活更简单”的服务承诺下，湖北分公司的销售队伍和理赔队伍坚守一线，用专业，用真诚服务客户，为客户排忧解难，提供极致服务体验。从 2003 年率先提出全国通赔，到 2009 年承诺“资料齐全、一万以下，三天赔付”，再到现在升级推出的省心省时又省钱的“一键包办”服务体系，持续提升客户理赔服务体验。

10、远江盛邦（北京）网络安全科技股份有限公司

远江盛邦（北京）网络安全科技股份有限公司（简称：盛邦安全）成立于 2010 年，专注于网络空间安全领域，以“让网络空间更有序”为使命，为客户提供网络安全基础类、业务场景安全类、网络空间地图类安全产品及服务。

公司核心产品的市场占有率多年来保持行业领先地位：根据 IDC 最新报告统计，盛邦安全漏洞扫描与

管理产品位居国内市场排名第三；WAF 产品连续三年市场份额国内排名前五。在溯源管理技术领域，盛邦安全被 IDC 评为中国态势感知市场主要厂商，先后获得 IDC“大数据安全”、“中国网络安全风险态势感知系统”创新者称号，并获得大数据协同安全技术国家工程实验室颁发的“大数据安全优秀案例奖”。

11、浙江远算科技有限公司

远算是国内领先的创新研发云平台产品与服务提供商，以云计算、大数据为支点，实现 HPC、3D 云应用、CAD/CAE 等技术融合，打造出服务于工业数字化转型的平台化产品组合。作为一家互联网属性的工业数字化研发平台，远算完美融合工业数字化与云计算黑科技，并携手西门子及全球领先的能源公司 EDF，以同步世界 500 强的发展速度撬动万亿级新基建市场。

公司自成立以来吸引了如 Facebook、微软、联想、IBM、北汽、阿里巴巴、富士康等海内外顶尖人才，组成了一支跨界融合、兼容并包的创新性团队。

12、上海三零卫士信息安全有限公司

上海三零卫士信息安全有限公司（以下简称三零卫士）成立于 2001 年 7 月 5 日，总部设在上海，在北京、成都、广州、杭州、武汉等地设有分支机构。公司是中国电子科技网络信息安全有限公司（简称中国网安）旗下专业从事网络安全服务的高新技术企业，现有员工 700 余人。公司重点聚焦党政机关、医卫、教育、能源、金融、交通等行业，为之提供基于信息系统全生命周期的信息安全服务，形成了网络安全服务、工业安全服务、数据安全服务、自主可控产品四大核心业务。作为国内最早从事网络安全服务的前瞻者和领军者，三零卫士已成为“国内领先、信息安全特色明显、IT 服务能力卓越”的综合性网络安全服务提供商。

公司长期参与国家、部委、地方政府的信息安全政策规划咨询，承担了国家 863 计划、国家创新基金、国家火炬计划、国家发改委高技术产业化、上海市科委科技攻关计划、上海市经信委等多项重大科研项目。在国家信息安全标准化工作中，公司作为主要执笔人和起草单位，承担和参与了国家、公安部、北京市、上海市、杭州市等 20 余项标准的制定工作。

13、汉口学院

汉口学院是经教育部批准设立的多学科、综合性民办普通本科高等学校。学校创立于 2000 年，其前身为华中师范大学汉口分校。2011 年经湖北省人民政府申报，教育部批准，转设并更名为汉口学院，是全国首批由独立学院转设为普通民办本科高校的 17 所高校之一。2014 年经省教育厅批准成为全省 32 所同类高校中率先进入二本招生高校，也是湖北省民办高校首批联合招收培养硕士研究生的高校之一。

学校设有 13 院 (含威尔士三一圣大卫大学汉口学院英国研究生院)1 部共 14 个教学单位，36 个本科专业，涵盖经济学、法学、教育学、文学、工学、管理学、艺术学等七大学科门类。现有全日制在校本专科生 1.4 万余人，其中本科生 11449 人。

学校师资力量雄厚，拥有一支教学经验丰富、学术水平较高，职称、学历、年龄结构合理的专任教师队伍。学校拥有湖北省重点学科 2 个，省级一流本科专业 7 个，省级专业综合改革试点项目 3 个，湖北省普通高校战略型龙头（支柱）产业人才培养计划项目 1 个，荆楚卓越工程师协同育人计划项目 1 个，计算机类专业 MOOC 教学试点高校项目 1 个，9 门省级重点课程，2 项省级教学成果奖，3 个省级教学团队，5 个省级优秀基层教学组织，同时承担省部级教研项目 83 项、教育部协同育人计划项目 72 项，在全省同类高校处于领先地位。

计算机科学与技术学院属于学校二级学院之一，成立于 2000 年，是学校最早设立的学院之一。 现有计算机科学与技术、电子商务、物联网工程、数字媒体技术 4 个本科专业和计算机应用技术、电子商务 2 个专科专业，电子商务和计算机科学与技术专业是湖北省一流本科专业。学院同时承担全校计算机公共课和数学公共课的教学。学院目前在校学生 2100 余人。

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