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

没有网络安全　就没有国家安全

There is no national security without network security.

公众号二维码

视频号二维码

地址：武汉市江汉区发展大道 164 号武汉科技大厦 605-1
电话：027—85519110　网址：www.whcsa.org.cn　邮箱 :hz@whcsa.org.cn

武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2025年第1期　总第5期

内部资料　电子样本

武汉市网络安全协会简介

INTRODUCTION TO WUHAN CYBER SECURITY ASSOCIATION

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

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

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

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

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

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

卷首语

人工智能（AI）正深刻重构社会生产与生活方式，其赋能医疗、金融等领域的效能有目共睹。然而技术跃升伴生的安全问题已跨越纯技术范畴，向伦理、法律及社会心理等维度蔓延：数据泄露与偏见削弱系统可信度，算法黑箱与鲁棒性不足引发决策风险，模型窃取与后门攻击威胁关键设施，而技术恶意滥用更可能加剧社会信任危机。这些交织的挑战警示我们：AI 安全是涵盖技术、伦理、法律、社会的系统工程，唯有筑牢安全基石，方能释放技术的真正价值。

面对多维安全挑战，需要凝聚全社会的共治力量。AI 安全治理的本质是平衡技术创新与风险控制的动态过程。在数据层面，需保障全生命周期安全；在算法层面，应提升透明性与鲁棒性；在应用层面，须防范模型被恶意利用。更重要的是，必须建立贯穿技术研发、部署应用、监管问责的全链条治理机制。这需要政府、企业、科研机构和社会各界的共同努力。尤其要强调：技术发展必须与安全治理同频共振——当医疗 AI 处理敏感数据时，需同步建立隐私计算屏障；当金融模型进行决策时，须同步消除算法歧视。只有通过多方共治，才能实现 AI" 可控发展 " 与 " 风险可控 " 的辩证统一。

作为推动武汉网络安全发展的重要力量，协会在此关键时期肩负特殊使命。我们呼吁全体成员单位：以技术创新筑牢安全底座，以行业自律引领发展航向。高校科研机构应聚焦隐私计算、对抗防御等关键技术攻关；企业需将内生安全理念融入产品研发全流程；专家智库要积极参与标准制定与政策咨询。在此呼吁各方紧密协同：通过共享威胁情报提升区域防护能力，通过人才联合培养补强安全队伍短板，通过制定行业公约规范技术应用边界。我们深信，在政产学研用的合力驱动下，武汉网络安全战线必将为 AI 技术健康发展提供坚实保障——让安全成为智能时代的温暖底色，使创新在有序轨道上行稳致远，最终实现技术造福人类的美好愿景。

武汉市网络安全协会专家委员会专家、

湖北大学网络空间安全学院副院长：何鹏

目 录

CATALOGUE

个人信息保护合规审计管理办法

第18号

《个人信息保护合规审计管理办法》已经 2024 年 5 月 20 日国家互联网信息办公室 2024 年第 15 次室务会会议审议通过，现予公布，自 2025 年 5 月 1 日起施行。

国家互联网信息办公室主任　庄荣文

2025 年 2 月 12 日

第一条 为了规范个人信息保护合规审计活动，保护个人信息权益，根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规，制定本办法。

第二条 在中华人民共和国境内开展个人信息保护合规审计，适用本办法。

本办法所称个人信息保护合规审计，是指对个人信息处理者的个人信息处理活动是否遵守法律、行政法规的情况进行审查和评价的监督活动。

第三条 个人信息处理者自行开展个人信息保护合规审计的，应当由个人信息处理者内部机构或者委托专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。

第四条 处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。

第五条 个人信息处理者有以下情形之一的，国家网信部门和其他履行个人信息保护职责的部门（以下统称为保护部门），可以要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计：

（一）发现个人信息处理活动存在严重影响个人权益或者严重缺乏安全措施等较大风险的；

（二）个人信息处理活动可能侵害众多个人的权益的；

（三）发生个人信息安全事件，导致 100 万人以上个人信息或者 10 万人以上敏感个人信息泄露、篡改、丢失、毁损的。

对同一个人信息安全事件或者风险，不得重复要求个人信息处理者委托专业机构开展个人信息保护合规审计。

第六条 个人信息处理者自行开展或者按照保护部门要求委托专业机构开展个人信息保护合规审计的，应当参照本办法附件《个人信息保护合规审计指引》。

第七条 专业机构应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等。

鼓励相关专业机构通过认证。专业机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

第八条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当为专业机构正常开展个人信息保护合规审计工作提供必要支持，并承担审计费用。

第九条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求选定专业机构，在限定时间内完成个人信息保护合规审计；情况复杂的，报保护部门批准后，可以适当延长。

第十条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，在完成合规审计后，应当将专业机构出具的个人信息保护合规审计报告报送保护部门。

个人信息保护合规审计报告应当由专业机构主要负责人、合规审计负责人签字并加盖专业机构公章。

第十一条 个人信息处理者按照保护部门要求开展个人信息保护合规审计的，应当按照保护部门要求对合规审计中发现的问题进行整改。在整改完成后 15 个工作日内，向保护部门报送整改情况报告。

第十二条 处理 100 万人以上个人信息的个人信息处理者应当指定个人信息保护负责人，负责个人信息处理者的个人信息保护合规审计工作。

提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当成立主要由外部成员组成的独立机构对个人信息保护合规审计情况进行监督。

第十三条 专业机构在从事个人信息保护合规审计活动时，应当遵守法律法规，诚信正直，公正客观地作出合规审计职业判断，对在履行个人信息保护合规审计职责中获得的个人信息、商业秘密、保密商务信息等应当依法予以保密，不得泄露或者非法向他人提供，在合规审计工作结束后及时删除相关信息。

第十四条 专业机构不得转委托其他机构开展个人信息保护合规审计。

第十五条 同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计。

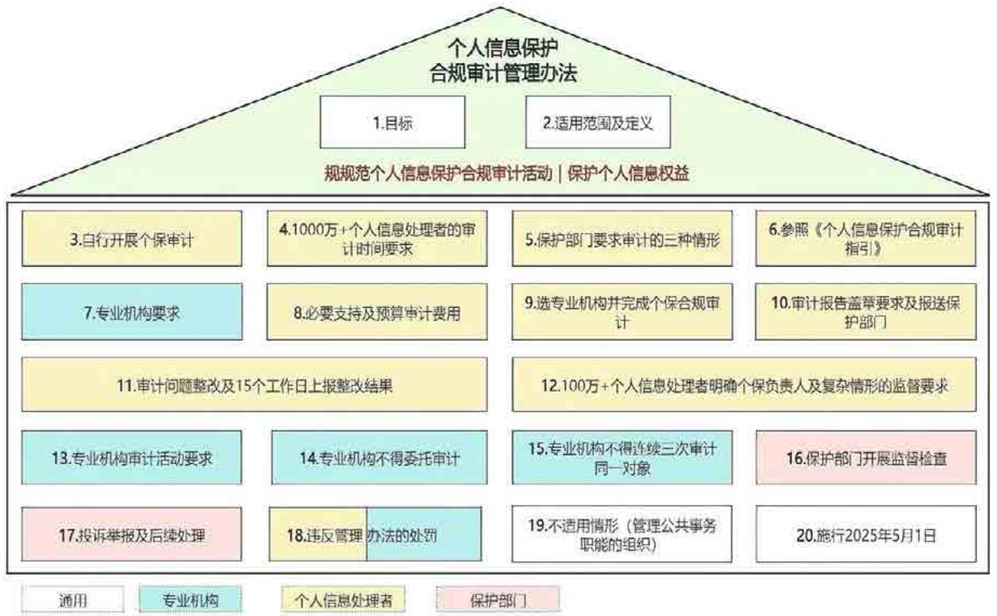
第十六条 保护部门对个人信息处理者开展个人信息保护合规审计情况进行监督检查。

第十七条 任何组织、个人有权对个人信息保护合规审计中的违法活动向保护部门进行投诉、举报。收到投诉、举报的部门应当依法及时处理，并将处理结果告知投诉、举报人。

第十八条 个人信息处理者、专业机构违反本办法规定的，依照《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律法规的规定处理；构成犯罪的，依法追究刑事责任。

第十九条 对国家机关和法律、法规授权的具有管理公共事务职能的组织的个人信息保护合规审计，不适用本办法。

第二十条 本办法自 2025 年 5 月 1 日起施行。



附件

个人信息保护合规审计指引

一、本指引根据《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规制定。

二、对个人信息处理活动的合法性基础进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人同意，该同意是否由个人在充分知情的前提下自愿、明确作出；

（二）基于个人同意处理个人信息的，个人信息的处理目的、处理方式、处理的个人信息种类发生变更的，是否重新取得个人同意；

（三）基于个人同意处理个人信息的，是否依照法律、行政法规取得个人单独同意或者书面同意；

（四）处理个人信息未取得个人同意的，是否属于法律、行政法规规定不需要取得个人同意的情形。

三、对个人信息处理规则进行合规审计的，应当重点审查下列事项：

（一）是否真实、准确、完整地告知个人信息处理者的名称或者姓名和联系方式；

（二）是否以清单等便于查看的形式列明所收集的个人信息及其处理方式和种类；

（三）是否与处理目的直接相关，采取对个人权益影响最小的方式；

（四）是否明确个人信息保存期限或者保存期限的确定方法、到期后的处理方式，以及确定保存期限为实现处理目的所必要的最短时间；

（五）是否明确个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的途径和方法。

四、对个人信息处理者履行告知个人信息处理规则义务进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在处理个人信息前，是否以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理规则；

（二）告知文本的大小、字体和颜色是否便于个人完整阅读告知事项；

（三）线下告知是否通过标注、说明等多种方式向个人履行告知义务；

（四）在线告知是否提供文本信息或者通过适当方式向个人履行告知义务；

（五）个人信息处理规则发生变更的，是否将变更内容及时告知个人；

（六）处理个人信息不需要告知的，是否属于法律、行政法规规定应当保密或者不需要告知的情形。

五、对个人信息处理者与其他个人信息处理者共同处理个人信息进行合规审计的，应当重点审查下列事项：

（一）是否约定各自的权利义务；

（二）个人信息权益保护机制；

（三）个人信息安全事件报告机制；

（四）其他法律、行政法规规定需要约定的权利和义务。

六、对个人信息处理者委托处理个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者在委托处理个人信息前，是否开展个人信息保护影响评估；

（二）个人信息处理者与受托人签订的合同，是否与受托人约定了委托处理的目的、期限、方式、个人信息的种类、保护措施以及双方的权利义务等；

（三）个人信息处理者是否采取定期检查等方式，对受托人的个人信息处理活动进行监督。

七、个人信息处理者存在因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息情形的，应当重点审查个人信息处理者是否向个人告知接收方的名称或者姓名和联系方式。

八、对个人信息处理者向其他个人信息处理者提供其处理的个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，是否取得个人的单独同意；

（二）是否向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，法律、行政法规规定应当保密或者不需要告知的除外；

（三）是否事前进行个人信息保护影响评估。

九、对个人信息处理者利用自动化决策处理个人信息进行合规审计的，应当重点审查下列事项：

（一）自动化决策的透明度，以及自动化决策的结果是否公平、公正；

（二）是否事前告知个人自动化决策处理个人信息的种类及可能带来的影响；

（三）是否事前进行个人信息保护影响评估；

（四）是否向用户提供保障机制，以便个人通过便捷方式拒绝通过自动化决策方式作出对个人权益有重大影响的决定，并要求个人信息处理者就通过自动化决策方式作出对用户个人权益有重大影响的决定予以说明；

（五）向个人进行信息推送、商业营销的，是否同时提供不针对个人特征的选项，或者提供便捷的拒绝自动化决策服务的方式；

（六）是否采取了有效措施，防止自动化决策根据消费者的偏好、交易习惯等对个人在交易条件上实行不合理的差别待遇；

（七）其他可能影响自动化决策的透明度和结果公平、公正的事项。

十、对个人信息处理者基于个人同意公开个人信息进行合规审计的，应当重点审查下列事项：

（一）个人信息处理者公开其处理的个人信息前是否取得个人单独同意，该授权是否真实、有效，是否存在违背个人意愿将个人信息予以公开的情况；

（二）个人信息处理者公开个人信息前，是否进行个人信息保护影响评估。

十一、个人信息处理者在公共场所安装图像收集、个人身份识别设备的，应当重点对其安装图像收集、个人信息身份识别设备的合法性及所收集个人信息的用途进行审查。审查内容包括但不限于：

（一）是否为维护公共安全所必需，是否为商业目的处理所收集的个人信息；

（二）是否设置了显著的提示标识；

（三）个人信息处理者所收集的个人图像、身份识别信息用于维护公共安全以外用途的，是否取得个人单独同意。

十二、对个人信息处理者处理已公开的个人信息进行合规审计的，应当重点审查个人信息处理者是否存在下列违法违规行为：

（一）向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的商业信息；

（二）利用已公开的个人信息从事网络暴力、传播网络谣言和虚假信息等活动；

（三）处理个人明确拒绝处理的已公开个人信息；

（四）对个人权益有重大影响，未取得个人同意；

（五）收集、留存或处理已公开个人信息的规模、时间或使用目的超出合理范围。

十三、对个人信息处理者处理敏感个人信息进行合规审计的，应当重点审查下列事项：

（一）基于个人同意处理个人信息的，处理生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息，是否事前取得个人的单独同意；

（二）基于个人同意处理个人信息的，处理不满十四周岁未成年人的个人信息，是否事前取得未成年人的父母或者其他监护人的同意；

（三）处理敏感个人信息的目的、方式、范围是否合法、正当、必要；

（四）是否在事前进行个人信息保护影响评估；

（五）是否向个人告知处理敏感个人信息的必要性以及对个人权益的影响，法律、行政法规规定应当保密或者不需要告知的除外；

（六）法律、行政法规规定应当取得书面同意的，是否取得书面同意；

（七）是否遵守法律、行政法规对处理敏感个人信息的限制性规定。

十四、对个人信息处理者处理不满十四周岁未成年人个人信息进行合规审计的，应当重点审查下列事项：

（一）是否制定专门的个人信息处理规则；

（二）是否向未成年人及其监护人告知未成年人个人信息的处理目的、处理方式、处理必要性，以及处理个人信息的种类、所采取的保护措施等，法律、行政法规规定不需要告知的除外；

（三）基于个人同意处理个人信息，是否存在强制要求未成年人或者其监护人同意处理非必要个人信息的行为。

十五、对个人信息处理者向境外提供个人信息进行合规审计的，应当重点审查下列事项：

（一）关键信息基础设施运营者向境外提供个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（二）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息是否经过国家网信部门组织的安全评估，法律、行政法规、国家网信部门另有规定的，从其规定；

（三）关键信息基础设施运营者以外的数据处理者自当年 1 月 1 日起累计向境外提供 10 万人以上、不满 100 万人个人信息（不含敏感个人信息）或者不满 1 万人敏感个人信息的，是否按照国家网信部门的规定，经个人信息保护认证或者按照国家网信部门制定的标准合同与境外接收方签订合同并向所在地省级网信部门备案，或者符合法律、行政法规、国家网信部门规定的其他条件；

（四）存在向外国司法或者执法机构提供存储于中华人民共和国境内个人信息情形的，是否经过中华人民共和国主管机关批准；

（五）是否向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息。

十六、对个人信息删除权保障情况进行合规审计的，应当重点审查下列事项：

（一）个人信息处理目的是否已实现、无法实现或者为实现处理目的不再必要；

（二）个人信息处理者是否停止提供产品或者服务，或者个人是否已注销账号；

（三）保存期限是否已届满；

（四）个人是否撤回同意；

（五）个人信息处理者是否违反法律、行政法规或者违反约定处理个人信息；

（六）应当删除个人信息，但法律、行政法规规定的保存期限未届满，或者删除个人信息从技术上难以实现的，个人信息处理者是否停止除存储和采取必要的安全措施之外的处理。

十七、对个人信息处理者保障个人在个人信息处理活动中的权利情况进行合规审计的，应当重点审查下列事项：

（一）是否建立便捷的个人行使权利的申请受理机制和处理机制；

（二）是否及时响应个人行使权利的申请，是否及时、完整、准确告知处理意见或者执行结果；

（三）拒绝个人行使权利请求的，是否向个人说明理由。

十八、个人信息处理者应当响应个人申请，对其个人信息处理规则进行解释说明，合规审计时应当重点对下列内容进行评价：

（一）个人信息处理者是否提供便捷的方式和途径，接受、处理个人关于个人信息处理规则解释说明的要求；

（二）接到个人的要求后，个人信息处理者是否在合理的时间内，使用通俗易懂的语言对其个人信息处理规则作出解释说明。

十九、个人信息处理者应当依照法律、行政法规的规定制定内部管理制度和操作规程，明确组织架构、岗位职责，建立工作流程、完善内控制度，保障个人信息处理合规与安全。合规审计时，应当重点对个人信息处理者个人信息保护内部管理制度和操作规程进行审查，包括但不限于：

（一）个人信息保护工作的方针、目标、原则是否符合法律、行政法规规定；

（二）个人信息保护组织架构、人员配备、行为规范、管理责任是否与应当履行的个人信息保护责任相适应；

（三）是否根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分类；

（四）是否建立个人信息安全事件应急响应机制；

（五）是否建立个人信息保护影响评估制度、合规审计制度；

（六）是否建立畅通的个人信息保护投诉举报受理流程；

（七）是否合理制定个人信息处理操作权限；

（八）是否制定实施个人信息保护安全教育和培训计划；

（九）是否建立个人信息保护负责人及相关人员履职评价制度；

（十）是否建立个人信息违法处理责任制度；

（十一）法律、行政法规规定的其他事项。

二十、个人信息处理者应当采取与所处理个人信息规模、类型相适应的安全技术措施，并对个人信息处理者采取的技术措施的有效性进行评价，评价内容包括但不限于：

（一）是否采取相应安全技术措施实现个人信息的保密性、完整性、可用性；

（二）是否采取加密、去标识化等安全技术措施，确保在不借助额外信息的情况下，消除或者降低个人信息的可识别性；

（三）采取的安全技术措施能否合理确定有关人员查阅、复制、传输个人信息等的操作权限，减少个人信息在处理过程中未经授权的访问和滥用风险。

二十一、对个人信息处理者教育培训计划的制定和实施情况进行合规审计时，应当重点对下列事项进行评价：

（一）是否按计划对管理人员、技术人员、操作人员、全员开展相应的安全教育和培训，是否对相应人员的个人信息保护意识和技能进行考核；

（二）培训内容、方式、对象、频率等能否满足个人信息保护需要。

二十二、对个人信息处理者指定的个人信息保护负责人履职情况进行合规审计的，应当重点审查下列事项：

（一）个人信息保护负责人是否具有相关的工作经历和专业知识，熟悉个人信息保护相关法律、行政法规；

（二）个人信息保护负责人是否具有明确清晰的职责，是否被赋予充分的权限协调个人信息处理者内部相关部门与人员；

（三）个人信息保护负责人在个人信息处理重大事项决策前是否有权提出相关意见和建议；

（四）个人信息保护负责人是否有权对个人信息处理者内部个人信息处理的不合规操作进行制止和采取必要的纠正措施；

（五）个人信息处理者是否公开个人信息保护负责人的联系方式，并将个人信息保护负责人的姓名、联系方式等报送保护部门。

二十三、对个人信息处理者开展个人信息保护影响评估情况进行合规审计时，应当重点对影响评估开展情况和评估内容进行审查：

（一）是否依照法律、行政法规的规定，在进行对个人权益具有重大影响的个人信息处理活动前进行个人信息保护影响评估；

（二）是否对个人信息的处理目的、处理方式等进行合法、正当、必要评估；

（三）是否对个人权益的影响及安全风险进行评估；

（四）是否对所采取的保护措施的合法性、有效性，以及与风险程度的适应性进行评估。

二十四、个人信息处理者应当制定个人信息安全事件应急预案。合规审计时，应当对应急预案的全面性、有效性、可执行性作出评价，包括但不限于下列内容：

（一）是否结合业务实际，对面临的个人信息安全风险作出系统评估和预测；

（二）总体要求、基本策略，组织机构、人员，技术、物资保障，指挥处置程序，应急和支持措施等是否足以应对预测的风险；

（三）是否对相关人员进行应急预案培训，定期对应急预案进行演练。

二十五、对个人信息处理者个人信息安全事件应急响应处置情况进行合规审计的，应当重点审查下列事项：

（一）是否按照应急预案、操作规程及时查明个人

信息安全事件的影响、范围和可能造成的危害，分析、确定事件发生的原因，提出防止危害扩大的措施方案；

（二）是否建立通报渠道，在安全事件发生后按照相关规定及时通知保护部门和个人；

（三）是否采取相应措施将个人信息安全事件可能造成的损失和可能产生的危害风险降低到最小。

二十六、对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者制定的平台规则进行合规审计的，应当重点审查下列事项：

（一）平台规则是否与法律、行政法规相抵触；

（二）平台规则个人信息保护条款的有效性，是否合理界定了平台、平台内产品或者服务提供者的个人信息保护权利和义务；

（三）平台规则的执行情况，是否通过抽样等方式验证平台规则被有效执行。

二十七、对提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者发布的个人信息保护社会责任报告进行合规审计的，应当重点审查社会责任报告披露下列内容的情况：

（一）个人信息保护组织架构和内部管理情况；

（二）个人信息保护能力建设情况；

（三）个人信息保护措施和成效；

（四）个人行使权利的申请受理情况；

（五）独立监督机构履职情况；

（六）重大个人信息安全事件处理情况；

（七）促进个人信息保护社会共治的科普宣传、公益活动情况；

（八）法律、行政法规规定的其他事项。

近日，国家互联网信息办公室公布《个人信息保护合规审计管理办法》（以下简称《办法》），自 2025 年 5 月 1 日起施行。

国家互联网信息办公室有关负责人表示，《中华人民共和国个人信息保护法》《网络数据安全管理条例》对个人信息处理者开展个人信息保护合规审计作了规定，《办法》对合规审计活动的开展、合规审计机构的选择、合规审计的频次、个人信息处理者和专业机构在合规审计中的义务等作出细化规定，旨在为个人信息处理者开展个人信息保护合规审计提供系统性、针对性、可操作性的规范，提升个人信息处理活动合法合规水平，保护个人信息权益。《办法》明确了个人信息处理者开展合规审计的两种情形。一是个人信息处理者自行开展合规审计的，应当由个人信息处理者内部机构或者委托专业机构定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。处理超过 1000 万人个人信息的个人信息处理者，应当每两年至少开展一次个人信息保护合规审计。二是履行个人信息保护职责的部门发现个人信息处理活动存在较大风险、可能侵害众多个人的权益或者发生个人信息安全事件的，可以要求个人信息处理者委托专业机构对个人信息处理活动进行合规审计。

《办法》明确了开展合规审计的个人信息处理者应当履行的义务。规定个人信息处理者按照履行个人信息保护职责的部门要求开展合规审计的，应当为专业机构正常开展合规审计工作提供必要支持并承担审计费用，在限定时间内完成合规审计，报送合规审计报告并进行整改。

《办法》明确了专业机构在合规审计中的义务。一是应当具备开展个人信息保护合规审计的能力，有与服务相适应的审计人员、场所、设施和资金等。二是应当遵守法律法规，诚信正直，公正客观地作出合规审计职业判断，对履职中知悉的个人信息、商业秘密、保密商务信息等依法予以保密。三是不得转委托其他机构开展个人信息保护合规审计。四是同一专业机构及其关联机构、同一合规审计负责人不得连续三次以上对同一审计对象开展个人信息保护合规审计。

《办法》以附件形式提供了《个人信息保护合规审计指引》，对个人信息保护相关法律、行政法规的关键要点作了梳理，从合规审计的角度进行了细化。个人信息处理者自行开展或者按照履行个人信息保护职责的部门要求委托专业机构开展个人信息保护合规审计，应当参照《个人信息保护合规审计指引》。

《办法》同时对履行个人信息保护职责的部门的监督管理责任和个人信息处理者、专业机构违反《办法》规定的法律责任等作出了规定。

李强签署国务院令 公布《政务数据共享条例》

中华人民共和国国务院令
第 809 号

《政务数据共享条例》已经 2025 年 5 月 9 日国务院第 59 次常务会议通过，现予公布，自 2025 年 8 月 1 日起施行。

总理 李强

2025 年 5 月 28 日

政务数据共享条例

第一章 总则

第一条 为了推进政务数据安全有序高效共享利用，提升政府数字化治理能力和政务服务效能，全面建设数字政府，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》等法律，制定本条例。

第二条 政府部门和法律、法规授权的具有管理公共事务职能的组织（以下统称政府部门）之间政务数据共享以及相关安全、监督、管理等工作，适用本条例。

第三条 本条例所称政务数据，是指政府部门在依法履行职责过程中收集和产生的各类数据，但不包括属于国家秘密、工作秘密的数据。

本条例所称政务数据共享，是指政府部门因依法履行职责需要，使用其他政府部门的政务数据或者为其他政府部门提供政务数据的行为。

第四条 政务数据共享工作应当坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，遵循统筹协调、标准统一、依法共享、合理使用、安全可控的原则。

第五条 开展政务数据共享工作，应当遵守法律法规，履行政务数据安全保护义务，不得危害国家安全、公共利益，不得损害公民、法人和其他组织的合法权益。

第六条 国家建立政务数据共享标准体系，推进政务数据共享工作标准化、规范化。

第七条 国家鼓励政务数据共享领域的管理创新、机制创新和技术创新，持续提升政务数据共享效率、应用水平和安全保障能力。

第二章 管理体制

第八条 各级人民政府应当加强对政务数据共享工作的组织领导。

国务院政务数据共享主管部门负责统筹推进全国政务数据共享工作。

县级以上地方人民政府政务数据共享主管部门负责统筹推进本行政区域内政务数据共享工作。

国务院各部门负责本部门政务数据共享工作，协调指导本行业、本领域政务数据共享工作。

第九条 政务数据共享主管部门应当会同其他政府部门研究政务数据共享中的重大事项和重要工作，总结、推广政务数据共享的典型案例和经验做法，协调推进跨层级、跨地域、跨系统、跨部门、跨业务政务数据安全有序高效共享利用。

第十条 政府部门应当落实政务数据共享主体责任，建立健全本部门政务数据共享工作制度，组织研究解决政务数据共享工作中的重大问题。

第十一条 政府部门应当明确本部门政务数据共享

工作机构。政务数据共享工作机构负责本部门政务数据共享具体工作，履行以下职责：

（一）组织编制、更新和维护本部门政务数据目录；

（二）组织提出本部门政务数据共享申请，组织审核针对本部门政务数据的共享申请，协调并共享本部门政务数据；

（三）确保本部门提供的政务数据符合政务数据共享标准规范；

（四）组织提出或者处理涉及本部门的政务数据校核申请；

（五）建立健全本部门政务数据共享中数据安全和个人信息保护制度，组织开展本部门政务数据共享安全性评估；

（六）本部门其他与政务数据共享相关的工作。

第三章 目录管理

第十二条 政务数据实行统一目录管理。国务院政务数据共享主管部门制定政务数据目录编制标准规范，组织编制国家政务数据目录。县级以上地方人民政府政务数据共享主管部门组织编制本行政区域内的政务数据目录。

政府部门应当依照本部门职责，按照政务数据目录编制标准规范，编制本部门政务数据目录。

第十三条 政府部门编制政务数据目录，应当依法开展保密风险、个人信息保护影响等评估，并经部门负责人审核同意。

政务数据目录应当明确数据目录名称、数据项、提供单位、数据格式、数据更新频率以及共享属性、共享方式、使用条件、数据分类分级等信息。

第十四条 政务数据按照共享属性分为无条件共享、有条件共享和不予共享三类：

（一）可以提供给所有政府部门共享使用的政务数据属于无条件共享类；

（二）可以按照一定条件提供给有关政府部门共享使用的政务数据属于有条件共享类；

（三）法律、行政法规以及国务院决定明确规定不能提供给其他政府部门共享使用的政务数据属于不予共享类。

第十五条 政府部门应当科学合理确定政务数据共享属性，不得通过擅自增设条件等方式阻碍、影响政务数据共享。

对属于有条件共享类的政务数据，政府部门应当在政务数据目录中列明共享范围、使用用途等共享使用条件。对属于不予共享类的政务数据，政府部门应当在政务数据目录中列明理由，并明确相应的法律、行政法规以及国务院决定依据。

第十六条 政府部门应当将编制的政务数据目录报送同级政务数据共享主管部门审核。政务数据共享主管部门审核通过后统一向政府部门通告。

政府部门应当对照统一发布的政务数据目录，丰富政务数据资源，保障政务数据质量，依法共享政务数据。

第十七条 政务数据目录实行动态更新。

因法律、行政法规、国务院决定调整或者政府部门职责变化导致政务数据目录需要相应更新的，政府部门应当自调整、变化发生之日起 10 个工作日内对政务数据目录完成更新，并报送同级政务数据共享主管部门审核。因特殊原因需要延长更新期限的，经同级政务数据共享主管部门同意，可以延长 5 个工作日。

政务数据共享主管部门应当自收到更新后的政务数据目录之日起 2 个工作日内完成审核并发布。

第四章 共享使用

第十八条 政府部门应当建立健全政务数据全过程质量管理体系，提高政务数据质量管理能力，加强政务数据收集、存储、加工、传输、共享、使用、销毁等标准化管理。

第十九条 政府部门应当按照法定的职权、程序和标准规范收集政务数据。通过共享获取政务数据能够满足履行职责需要的，政府部门不得向公民、法人和其他组织重复收集。

政务数据收集工作涉及多个政府部门的，政务数据共享主管部门应当明确牵头收集的政府部门并将其作为数源部门。数源部门应当加强与其他有关政府部门的协同配合、信息沟通，及时完善更新政务数据，保障政务数据的完整性、准确性和可用性，并统一提供政务数据共享服务。

第二十条 政务数据共享主管部门应当建立政务数据共享供需对接机制，明确工作流程。

政务数据需求部门应当根据履行职责需要，按照统一发布的政务数据目录，经本部门政务数据共享工作机构负责人同意后，依法提出政务数据共享申请，明确使用依据、使用场景、使用范围、共享方式、使用时限等，并保证政务数据共享申请的真实性、合法性和必要性。

政务数据提供部门应当按照本条例第二十一条规定的期限对政务数据需求部门提出的政务数据共享申请进行审核，经本部门政务数据共享工作机构负责人同意后作出答复。

第二十一条 政务数据需求部门申请共享的政务数据属于无条件共享类的，政务数据提供部门应当自收到政务数据共享申请之日起 1 个工作日内作出答复；属于有条件共享类的，应当自收到政务数据共享申请之日起 10 个工作日内作出是否同意共享的答复。因特殊原因需要延长答复期限的，政务数据提供部门应当报经同级政务数据共享主管部门同意，并告知政务数据需求部门，延长的期限最长不得超过 10 个工作日。

政务数据需求部门提交的申请材料不全的，政务数据提供部门应当一次性告知其需要补充的材料，不得直接予以拒绝。政务数据提供部门不同意共享的，应当说明理由。

第二十二条 政务数据提供部门应当自作出同意共享的答复之日起 20 个工作日内共享政务数据。

政务数据提供部门可以通过服务接口、批量交换、文件下载等方式向政务数据需求部门共享政务数据。

第二十三条 国家鼓励各级政府部门优化政务数据共享审核流程，缩短审核和提供共享政务数据的时间。

第二十四条 上级政府部门应当根据下级政府部门履行职责的需要，在确保政务数据安全的前提下，及时、完整回流业务信息系统收集和产生的下级政府行政区域内的政务数据，并做好系统对接和业务协同，不得设置额外的限制条件。

下级政府部门获得回流的政务数据后，应当按照履行职责的需要共享、使用，并保障相关政务数据安全。

第二十五条 政府部门通过共享获得政务数据的，不得擅自扩大使用范围以及用于或者变相用于其他目的，不得擅自将获得的政务数据提供给第三方。确需扩大使用范围、用于其他目的或者提供给第三方的，应当经政务数据提供部门同意。

政务数据共享主管部门以及其他政府部门应当采取措施防范政务数据汇聚、关联引发的泄密风险。

第二十六条 国务院政务数据共享主管部门应当统筹建立政务数据校核纠错制度。

政府部门应当依照本部门职责，建立政务数据校核纠错规则，提供纠错渠道。政务数据需求部门应当记录政务数据使用状态，发现政务数据不准确或者不完整的，应当及时向政务数据提供部门提出政务数据校核申请。政务数据提供部门应当自收到政务数据校核申请之日起 10 个工作日内予以核实、更正并反馈校核处理结果。

第二十七条 政务数据需求部门通过共享获取的政务数据，共享目的已实现、无法实现或者为实现共享目的不再必要的，应当按照政务数据提供部门的要求妥善处置。

政务数据需求部门存在擅自超出使用范围、共享目的使用政务数据，或者擅自将政务数据提供给第三方的，政务数据共享主管部门或者政务数据提供部门应当暂停其政务数据共享权限，并督促限期整改，对拒不整改或者整改不到位的，可以终止共享。

政务数据提供部门无正当理由，不得终止或者变更已提供的政务数据共享服务。确需终止或者变更服务的，政务数据提供部门应当与政务数据需求部门协商，并报同级政务数据共享主管部门备案。

第二十八条 政务数据共享主管部门应当建立健全政务数据共享争议解决处理机制。

同级政务数据需求部门、政务数据提供部门发生政

务数据共享争议的，应当协商解决；协商不成的，应当按照程序向同级政务数据共享主管部门申请协调处理。跨层级、跨地域的政务数据共享发生争议的，由共同的上级政务数据共享主管部门协调处理。经政务数据共享主管部门协调处理仍未达成一致意见的，报政务数据共享主管部门的本级人民政府决定。

第二十九条 政务数据共享主管部门应当对政务数据共享情况进行监督检查，并可以对违反本条例规定的行为予以通报。

政务数据需求部门应当对共享政务数据的使用场景、使用过程、应用成效、存储情况、销毁情况等进行记录，有关记录保存期限不少于 3 年。政务数据共享主管部门和政务数据提供部门可以查阅政务数据需求部门有关记录。法律、行政法规另有规定的，从其规定。

第五章 平台支撑

第三十条 国家统筹数据基础设施建设，提高政务数据安全防护能力，整合构建标准统一、布局合理、管理协同、安全可靠的全国一体化政务大数据体系。

国务院政务数据共享主管部门统筹全国一体化政务大数据体系的建设和管理工作，负责整合构建国家政务大数据平台，实现与国务院有关部门政务数据平台、各地区政务数据平台互联互通，为政务数据共享提供平台支撑。

县级以上地方人民政府政务数据共享主管部门负责本行政区域政务数据平台建设和管理工作，按需向乡镇（街道）、村（社区）共享政务数据。

国务院有关部门负责建设、优化本部门政务数据平台，可以支撑本行业、本领域的政务数据共享工作。未建设政务数据平台的，可以通过国家政务大数据平台开展本部门政务数据共享工作。

第三十一条 政府部门已建设的政务数据平台应当纳入全国一体化政务大数据体系。除法律、行政法规另有规定外，原则上不得通过新建政务数据共享交换系统开展跨层级、跨地域、跨系统、跨部门、跨业务的政务数据共享工作。

第三十二条 政府部门应当通过全国一体化政务大数据体系开展政务数据共享相关工作。

第三十三条 国家鼓励和支持大数据、云计算、人工智能、区块链等新技术在政务数据共享中的应用。

第六章 保障措施

第三十四条 政务数据共享主管部门应当会同同级网信、公安、国家安全、保密行政管理、密码管理等部门，根据数据分类分级保护制度，推进政务数据共享安全管理制度建设，按照谁管理谁负责、谁使用谁负责的原则，明确政务数据共享各环节安全责任主体，督促落实政务数据共享安全管理责任。

政务数据需求部门在使用依法共享的政务数据过程中发生政务数据篡改、破坏、泄露或者非法利用等情形的，应当承担安全管理责任。

第三十五条 政府部门应当建立健全政务数据共享安全管理制度，落实政务数据共享安全管理主体责任和政务数据分类分级管理要求，保障政务数据共享安全。

政府部门应当采取技术措施和其他必要措施，防止政务数据被篡改、破坏、泄露或者非法获取、非法利用。

政府部门应当加强政务数据安全风险监测，发生政务数据安全事件时，立即启动应急预案，采取相应的应急处置措施，防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告。

第三十六条 政府部门委托他人参与建设、运行、维护政府信息化项目，存储、加工政务数据，应当按照国家有关规定履行批准程序，明确工作规范和标准，并采取必要技术措施，监督受托方履行相应的政务数据安全保护义务。受托方应当依照法律、行政法规的规定和合同约定履行政务数据安全保护义务，不得擅自访问、获取、留存、使用、泄露或者向他人提供政务数据。

政务数据平台建设管理单位应当依照法律、行政法规的规定和国家标准的强制性要求，保障平台安全、稳定运行，维护政务数据安全。

第三十七条 政府部门及其工作人员在开展涉及个人信息的政务数据共享活动时，应当遵守《中华人民共和国个人信息保护法》、《网络数据安全管理条例》等法律、行政法规的规定。

公民、法人和其他组织有权对政务数据共享过程中侵犯其合法权益的行为进行投诉、举报，接到投诉、举报的政府部门应当按照规定及时处理。

第三十八条 县级以上人民政府应当将政务数据共享工作所需经费列入本级预算。县级以上人民政府及其有关部门应当对政务数据共享相关经费实施全过程预算绩效管理。政务数据共享情况应当作为确定政府信息化项目建设投资、运行维护经费和项目后评价结果的重要依据。

政务数据共享主管部门应当加强对本行政区域内政务数据提供部门数据共享及时性和数据质量情况、政务数据需求部门数据应用情况和安全保障措施等的监督，并向本级人民政府报告。

第七章 法律责任

第三十九条 政务数据提供部门违反本条例规定，有下列情形之一的，由同级政务数据共享主管部门责令改正；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：

（一）未按照要求编制或者更新政务数据目录；

（二）通过擅自增设条件等方式阻碍、影响政务数据共享；

（三）未配合数源部门及时完善更新政务数据；

（四）未按时答复政务数据共享申请或者未按时共享政务数据，且无正当理由；

（五）未按照规定将业务信息系统收集和产生的下级政府行政区域内的政务数据回流至下级政府部门；

（六）收到政务数据校核申请后，未按时核实、更正；

（七）擅自终止或者变更已提供的政务数据共享服务；

（八）未按照规定将已建设的政务数据平台纳入全国一体化政务大数据体系；

（九）违反本条例规定的其他情形。

第四十条 政务数据需求部门违反本条例规定，有下列情形之一的，由同级政务数据共享主管部门责令改正；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：

（一）重复收集可以通过共享获取的政务数据；

（二）擅自超出使用范围、共享目的使用通过共享获取的政务数据；

（三）擅自将通过共享获取的政务数据提供给第三方；

（四）共享目的已实现、无法实现或者为实现共享目的不再必要，未按照要求妥善处置通过共享获取的政务数据；

（五）未按照规定保存通过共享获取的政务数据有关记录；

（六）未对通过共享获取的政务数据履行安全管理责任；

（七）违反本条例规定的其他情形。

第四十一条 政务数据共享主管部门违反本条例规定，有下列情形之一的，由本级人民政府或者上级主管部门责令改正；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：

（一）未按照规定明确数源部门；

（二）未按照规定对政务数据共享争议进行协调处理；

（三）违反本条例规定的其他情形。

第四十二条 政府部门及其工作人员泄露、出售或者非法向他人提供政务数据共享工作过程中知悉的个人隐私、个人信息、商业秘密、保密商务信息的，或者在政务数据共享工作中玩忽职守、滥用职权、徇私舞弊的，依法给予处分；构成犯罪的，依法追究刑事责任。

第八章 附则

第四十三条 国家推动政府部门与其他国家机关参照本条例规定根据各自履行职责需要开展数据共享。

第四十四条 本条例自 2025 年 8 月 1 日起施行。

国家网络身份认证公共服务管理办法

中华人民共和国公安部
国家互联网信息办公室
中华人民共和国民政部
中华人民共和国文化和旅游部
国家卫生健康委员会
国家广播电视总局
令
第 173 号

《国家网络身份认证公共服务管理办法》已经2025年2月27日第1次公安部部务会议审议通过，并经国家互联网信息办公室、民政部、文化和旅游部、国家卫生健康委员会、国家广播电视总局同意，现予公布，自 2025 年 7 月 15 日起施行。

中华人民共和国公安部部长 王小洪
国家互联网信息办公室主任 庄荣文
中华人民共和国民政部部长 陆治原
中华人民共和国文化和旅游部部长 孙业礼
国家卫生健康委员会主任 雷海潮
国家广播电视总局局长 曹淑敏
2025 年 5 月 19 日

国家网络身份认证公共服务管理办法

第一条 为实施可信数字身份战略，推进国家网络身份认证公共服务建设，保护公民身份信息安全，支撑数字经济健康有序发展，根据《网络安全法》、《数据安全法》、《个人信息保护法》、《反电信网络诈骗法》、《未成年人保护法》等法律法规，制定本办法。

第二条 本办法所称国家网络身份认证公共服务（以下简称“公共服务”），是指国家根据法定身份证件信息，依托国家统一建设的网络身份认证公共服务平台（以下简称“公共服务平台”），为自然人提供申领网号、网证以及进行身份核验等服务。

本办法所称网号，是指与自然人身份信息相对应，由字母和数字组成、不含明文身份信息的网络身份符号；网证，是指承载网号及自然人非明文身份信息的网络身份认证凭证。网号、网证可用于在互联网服务及有关部门、行业管理、服务中非明文登记、核验自然人真实身份信息。

第三条 国务院公安部门、国家网信部门会同国务院民政、文化和旅游、卫生健康、广播电视等部门依照本办法和有关法律、行政法规的规定，在各自职责范围内负责网络身份认证公共服务有关工作。

第四条 持有有效法定身份证件的自然人，可以自愿向公共服务平台申领网号、网证。

不满十四周岁的自然人申领网号、网证的，应当取得其父母或者其他监护人同意，并由其父母或者其他监护人代为申领。

已满十四周岁未满十八周岁的自然人申领网号、网证的，应当在其父母或者其他监护人的监护下申领。

第五条 根据法律、行政法规规定，在互联网服务中需要登记、核验用户真实身份信息的，可以使用网号、网证依法进行登记、核验。

不满十四周岁的自然人使用网号、网证登记、核验真实身份信息的，应当取得其父母或者其他监护人同意。

第六条 鼓励有关主管部门、重点行业按照自愿原则推广应用网号、网证，为用户提供安全、便捷的身份登记和核验服务，通过公共服务培育网络身份认证应用生态。

有关主管部门、重点行业在管理、服务中，应当保留、提供现有的或者其他合法方式进行登记、核验真实身份。

第七条 鼓励互联网平台按照自愿原则接入公共服务，用以支持用户使用网号、网证登记、核验用户真实身份信息，依法履行个人信息保护和核验用户真实身份信息的义务。

互联网平台接入公共服务后，用户选择使用网号、网证登记、核验真实身份信息并通过验证的，互联网平台不得要求用户另行提供明文身份信息，法律、行政法规另有规定或者用户同意提供的除外。

互联网平台应当保障未使用网号、网证但通过其他方式登记、核验真实身份的用户与使用网号、网证的用户享有同等服务。

第八条 互联网平台需要依法核验用户真实身份信息但无需留存用户法定身份证件信息的，公共服务平台应当仅提供用户身份核验结果。

根据法律、行政法规规定，互联网平台确需获取、留存用户法定身份证件信息的，经用户授权或者单独同意，公共服务平台应当按照最小化原则提供。

未经自然人单独同意，互联网平台不得擅自处理或者对外提供相关数据、信息，法律、行政法规另有规定的除外。

第九条 公共服务平台仅限收集网络身份认证所必需的信息，处理个人信息或者向自然人提供公共服务，应当依法履行告知义务并取得其同意。处理敏感个人信息，应当取得个人的单独同意，法律、行政法规规定应当取得书面同意的，从其规定。

未经自然人单独同意，公共服务平台不得擅自处理或者对外提供相关数据、信息，不得将相关数据用于用户登记、核验真实身份以外的目的，法律、行政法规另有规定的除外。

公共服务平台应当依照法律、行政法规规定或者用户要求，及时删除用户个人信息。

第十条 涉及未成年人、老年人等用户的，公共服务平台可以依法向互联网平台提供年龄标识信息，用于支持互联网平台履行相应的法律义务。

第十一条 公共服务平台在处理用户个人信息前，应当通过用户协议等书面形式，以显著方式、清晰易懂的语言真实、准确、完整地向用户告知下列事项：

（一）公共服务平台的名称和联系方式；

（二）用户个人信息的处理目的、处理方式，处理的个人信息种类、保存期限；

（三）用户依法行使其个人信息相关权利的方式和程序；

（四）法律、行政法规规定应当告知的其他事项。

处理敏感个人信息的，还应当向个人告知处理的必要性以及对个人权益的影响，法律另有规定的除外。

公共服务平台处理个人信息，有法律、行政法规规定应当保密或者不需要告知的情形的，可以不向个人告知本条第一款规定的事项。

紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的，公共服务平台应当在紧急情况消除后及时告知。

第十二条 公共服务平台应当加强网络运行安全、数据安全和个人信息保护，建立并落实安全管理制度与技术防护措施，完善监督制度，有效保护网络运行安全、数据安全和个人信息权益。

公共服务平台处理的重要数据和个人信息应当在境内存储；因业务需要确需向境外提供的，应当按照国家有关规定进行安全评估。

公共服务平台发生网络运行安全、数据安全事件的，应当按照国家有关规定，立即启动应急预案，采取必要措施消除安全隐患，及时告知用户并向有关部门报告。

第十三条 公共服务平台的建设和服务涉及密码的，应当符合国家密码管理有关要求。

第十四条 违反本办法第七条、第八条、第九条、第十一条、第十二条规定，依照《网络安全法》、《数据安全法》、《个人信息保护法》，由国务院公安部门、国家网信部门在各自职责范围内依法予以处罚、处分；构成犯罪的，依法追究刑事责任。有关主管部门、重点行业在网络身份认证公共服务有关工作中玩忽职守、滥用职权的，依法追究责任。

第十五条 本办法所称法定身份证件，包括居民身份证、定居国外的中国公民的护照、港澳居民来往内地通行证、台湾居民来往大陆通行证、港澳居民居住证、台湾居民居住证、外国人永久居留身份证等身份证件。

第十六条 本办法自 2025 年 7 月 15 日起施行。

市场监管总局印发《网络交易合规数据报送管理暂行办法》（附全文）

近日，市场监管总局印发《网络交易合规数据报送管理暂行办法》（以下简称《办法》），规范网络交易合规数据报送行为，发挥数据在平台经济治理中的关键要素作用，引导平台企业合规经营，提升网络交易监管效能，促进平台经济健康发展。

《办法》共二十一条，主要内容包括 4 个方面：**一是明确网络交易合规数据范围。**明确为产生于境内的网络交易经营者身份信息、违法行为线索数据、行政执法协查数据、特定商品或者服务交易数据等网络交易监管相关数据。**二是规范网络交易合规数据报送行为。**明确 4 类数据的报送时限、报送层级和报送内容。**三是规范网络交易合规数据的利用和管理。**明确各级市场监管部门可以将网络交易合规数据依法用于监管执法和大数据综合分析应用，应依法保障数据安全并对履职中知悉的数据保密。**四是支持政务数据服务与社会共治。**明确总局将根据有关规定或标准提供政务数据服务。鼓励社会各方合法利用网络交易合规数据参与网络市场治理。

市场监管总局将以《办法》出台为契机，进一步营造稳定透明可预期的政策环境，指导平台企业落实合规数据报送主体责任，探索开展穿透式监管，持续推动提升平台经济常态化监管能力和水平，构建平台经济良好发展生态。

国家市场监督管理总局文件

国市监网监规〔2025〕2号

市场监管总局关于印发《网络交易合规数据报送管理暂行办法》的通知

各省、自治区、直辖市和新疆生产建设兵团市场监管局（厅、委）：

《网络交易合规数据报送管理暂行办法》已经2025年3月17日市场监管总局第5次局务会议通过。现印发给你们，请结合实际认真贯彻落实。

（此件公开发布）

— 1 —

网络交易合规数据报送管理暂行办法

第一条 为了规范网络交易合规数据报送和管理活动，提高网络交易监管效能，促进平台经济持续健康发展，根据《电子商务法》《网络安全法》《数据安全法》《个人信息保护法》《网络交易监督管理办法》等有关法律法规规章，制定本办法。

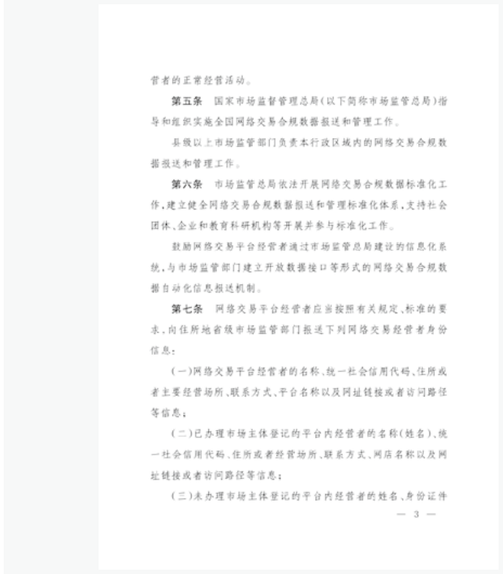
第二条 中华人民共和国境内的网络交易平台经营者向市场监管部门报送产生于中华人民共和国境内的网络交易合规数据，以及市场监管部门对网络交易合规数据报送进行管理、适用本办法。

第三条 本办法所称网络交易合规数据，是指网络交易平台经营者依据《电子商务法》《网络交易监督管理办法》向市场监管部门提供的，产生于中华人民共和国境内的网络交易经营者身份信息、违法行为线索数据、行政执法协查数据、特定商品或者服务交易数据等网络交易监管相关数据。

前款所称网络交易平台经营者包括为经营者提供网络经营场所、商品浏览、订单生成、在线支付等网络交易平台服务的网络社交、网络直播等网络服务提供者。

第四条 网络交易合规数据报送应当统筹发展与安全，坚持依法、必要原则，保护网络交易经营者和消费者合法权益，保守商业秘密，保护个人隐私，不得干扰网络交易平台经营者和平台内经

— 2 —



管者的正常经营活动。

第五条 国家市场监督管理总局（以下简称市场监管总局）指导和组织实施全国网络交易合规数据报送和管理工作。

县级以上市场监管部门负责本行政区域内的网络交易合规数据报送和管理工作。

第六条 市场监管总局依法开展网络交易合规数据标准化工作，建立健全网络交易合规数据报送和管理标准化体系，支持社会团体、企业和教育科研机构等开展并参与标准化工作。

鼓励网络交易平台经营者通过市场监管总局建设的信息化系统，与市场监管部门建立开放数据接口等形式的网络交易合规数据自动化信息报送机制。

第七条 网络交易平台经营者应当按照有关规定、标准的要求，向住所地省级市场监管部门报送下列网络交易经营者身份信息：

（一）网络交易平台经营者的名称、统一社会信用代码、住所或者主要经营场所、联系方式、平台名称以及网址链接或者访问路径等信息；

（二）已办理市场主体登记的平台内经营者的名称（姓名）、统一社会信用代码、住所或者经营场所、联系方式、网店名称以及网址链接或者访问路径等信息；

（三）未办理市场主体登记的平台内经营者的姓名、身份证件

号码、实际经营地址、联系方式、网店名称以及网址链接或者访问路径文字描述，属于依法不需要办理市场主体登记的具体情形的自我声明等数据；其中，对本平台内年交易额累计超过10万元额度的平台内经营者进行特别标示，并督促其及时依法办理市场主体登记。

第八条 网络交易平台经营者对平台内经营者违反市场监管法律、法规、规章的违法行为，应当自决定作出警示、暂停或者终止服务等处理措施之日起5个工作日内向住所地县级以上市场监管部门报告，报送平台内经营者身份信息、网店名称、商品或者服务信息、违法行为描述、保存的有关记录、处置措施等违法行为线索数据。

第九条 网络交易平台经营者应当在市场监管部门依法开展案件调查、事故处置、缺陷消费品召回、消费争议处理等执法活动时，按《网络交易执法协查暂行办法》要求提供平台内经营者身份信息、商品或者服务信息、支付记录、物流快递、退换货以及售后等交易数据。

第十条 网络交易平台经营者应当按照市场监管总局及其授权的省级市场监管部门的要求，提供特定时段、特定品类、特定区域的商品或者服务的价格、销量、销售额等交易数据。

第十一条 市场监管部门发现网络交易平台经营者报送或者提供的网络交易合规数据不准确或者不完整的，可以要求网络交

易平台经营者于5个工作日内更正、补充。

网络交易平台经营者发现提供的数据需要更正、补充的，应当自发现之日起5个工作日内，向市场监管部门申请更正、补充。

第十二条 市场监管部门以自动化监测等方式对网络交易平台公示展示的信息数据进行检查，网络交易平台经营者应当配合。

第十三条 市场监管总局可以将注册的网络交易经营者身份信息、违法行为线索数据、行政执法协查数据访问权限向网络交易经营者所在地县级以上市场监管部门开放。

第十四条 市场监管部门可以将网络交易平台经营者报送或者提供的网络交易合规数据依法用于监管执法活动。

市场监管部门可以按照国家有关规定对网络交易合规数据进行大数据综合分析应用，以支撑市场监管、政务服务等工作。

市场监管部门不得超越法定职权范围利用网络交易合规数据。

第十五条 各级市场监管部门应当严格遵守网络安全、数据安全、个人信息保护、保密等相关法律法规规定，依法保障个人信息权益和网络交易合规数据安全。

各级市场监管部门应当采取必要措施对在履行职责中知悉的个人隐私、个人信息、商业秘密、保密商务信息等数据依法予以保密，不得泄露或者非法向他人提供。

第十六条 自然人、法人和非法人组织认为市场监管部门的网络交易合规数据处理活动侵犯其个人信息、商业秘密等合法权益的，可以依法申请行政复议或者提起行政诉讼。

第十七条 市场监管总局可以根据有关规定或者标准，按要求向鼓励数据开放和授权运营、依法合规向网络交易平台经营者提供政务数据服务，支持网络交易平台经营者更好地开展平台内经营者身份核实，许可信息验证、信用体系建设和平台内治理等工作。

第十八条 鼓励企业、行业组织、科研机构等参与网络市场治理，推动网络交易合规数据合法、安全、有效利用。

就涉网络交易平台经营者之间运用违法行为线索数据等开展网络市场治理合作，对平台内经营者违法行为实施协同治理。

第十九条 网络交易平台经营者未依法报送网络交易经营者身份信息的，依照《电子商务法》第八十条的规定处罚。

网络交易平台经营者未依法报送违法行为线索数据、行政执法协查数据，特定商品或者服务交易数据的，会同依照《网络交易监管管理办法》第四十九条、第五十三条、第四十六条的规定处罚。

第二十条 通过自建网站、其他网络服务销售商品或者提供服务的网络交易经营者参照本办法执行。

第二十一条 本办法自2025年4月25日起施行。

市场监管总局办公厅　　2025年3月25日印发

《中华人民共和国网络安全法（修正草案再次征求意见稿）》

为了做好《中华人民共和国网络安全法》与相关法律的衔接协调，完善法律责任制度，保护个人、组织在网络空间的合法权益，维护国家安全和公共利益，根据《十四届全国人大常委会立法规划》，我办会同相关部门进一步研究起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》，现向社会公开征求意见。公众可通过以下途径和方式反馈意见：1. 通过电子邮件将意见发送至：law@cac.gov.cn。2. 通过信函将意见寄至：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法治局，邮编：100044，并在信封上注明“《网络安全法》意见”。意见反馈截止时间为 2025 年 4 月 27 日。

附件：1. 中华人民共和国网络安全法（修正草案再次征求意见稿）

2.关于《中华人民共和国网络安全法（修正草案再次征求意见稿）》的说明

国家互联网信息办公室

2025年3月28日

中华人民共和国网络安全法（修正草案再次征求意见稿）

一、将第五十九条修改为：“网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、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五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，由有关主管部门处二百万元以上一千万元以下罚款，并责令暂停相关业务、停业整顿、关闭网站或者应用程序、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处二十万元以上一百万元以下罚款。”

二、增加一条，作为第六十一条：“违反本法第二十三条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管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；违法所得十万元以上的，可以并处违法所得一倍以上三倍以下罚款；没有违法所得或者违法所得不足十万元的，可以并处三万元以上十万元以下罚款。”

三、增加一条，作为第六十四条：“有本法第六十

条第一项、第二项和第六十三条行为，造成本法第五十九条第三款规定的后果的，依照该款规定处罚。”

四、将第六十五条改为第六十七条，修改为：“关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、消除对国家安全的影响，并处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

五、将第六十八条、第六十九条第一项合并，作为第六十九条，修改为：“网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告的，或者违反本法第五十条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、通报批评，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、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五万元以上二十万元以下罚款。网络运营者有前款规定的违法行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、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二十万元以上一百万元以下罚款。电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前两款规定处罚。”

六、将第六十四条第一款、第六十六条、第七十条合并，作为第七十一条，修改为：“有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：（一）发布或者传输本法第十二条第二款和其他法律、行政法规禁止发布或者传输的信息的；（二）违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的；（三）违反本法第三十七条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。”

七、增加一条，作为第七十二条：“网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依照《中华人民共和国行政处罚法》的规定从轻、减轻或者不予行政处罚。有关主管部门依据职责制定相应的行政处罚裁量基准，规范行使行政处罚裁量权。”

八、对部分条文作以下修改：（一）将第六十一条改为第六十二条、第六十二条改为第六十三条，将其中的“关闭网站”修改为“关闭网站或者应用程序”。（二）将第六十四条第二款改为第六十六条。此外，对条文序号作了相应调整。

原《网络安全法》第59条	修订后
网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处~~一万元以上十万元~~以下罚款，对直接负责的主管人员处~~五千元以上五万元~~以下罚款。 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。	网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，**可以处一万元以上五万元以下罚款**；拒不改正或者导致危害网络安全等后果的，处**五万元以上五十万元**以下罚款，对直接负责的主管人员处~~一万元以上十万元~~以下罚款。 关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，**可以处五万元以上十万元**以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。 **有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、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五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，由有关主管部门处二百万元以上一千万元以下罚款，并责令暂停相关业务、停业整顿、关闭网站或者应用程序、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处二十万元以上一百万元以下罚款。**

关于《中华人民共和国网络安全法（修正草案再次征求意见稿）》的说明

党中央高度重视维护国家网络安全。习近平总书记多次作出重要指示，强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”。党的二十大和二十届三中全会对加强重点领域、新兴领域、涉外领域立法和增强立法系统性、整体性、协同性、时效性等作出了重要部署。为贯彻党中央决策部署，落实《十四届全国人大常委会立法规划》，适应网络安全新形势，我办会同相关部门起草了《中华人民共和国网络安全法（修正草案再次征求意见稿）》（以下简称《网络安全法（修正草案再次征求意见稿）》）。有关情况说明如下。

一、修改背景

《网络安全法》自2017年施行以来，为维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，提供了有力的法律保障。随着网络和信息技术日益融入社会生产生活，网络安全风险进一步凸显。2021年以来，《中华人民共和国数据安全法》（以下简称《数据安全法》）、《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）等网络安全相关立法相继制定实施，《中华人民共和国行政处罚法》（以下简称《行政处罚法》）修订出台，《网络安全法》需要适应形势加强与新出台法律的衔接协

原《网络安全法》第68条、69条第（一）项	修订后
网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告，没收违法所得；拒不改正或者情节严重的，处~~十万元以上五十万元~~以下罚款，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，对直接负责的主管人员和其他直接责任人员处~~一万元以上十万元~~以下罚款。 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前款规定处罚。	网络运营者违反本法第四十七条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告的，或者违反本法第五十条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、**通报批评**，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处**五十万元以上二百万元**以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站**或者应用程序**、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**五万元以上二十万元**以下罚款。 **网络运营者有前款规定的违法行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、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二十万元以上一百万元以下罚款。** 电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第四十八条第二款规定的安全管理义务的，依照前两款规定处罚。
网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款： （一）不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息，采取停止传输、消除等处置措施的； （……）	

原《网络安全法》第65条	修订后
关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令**停止使用**，处采购金额一倍以上十倍以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。	关键信息基础设施的运营者违反本法第三十五条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令**限期改正、消除对国家安全的影响**，并处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

调，对相关法律责任制度作出科学优化，进一步保障网络安全。2023年9月，《十四届全国人大常委会立法规划》发布，明确将“网络安全法（修改）”列入了“第一类项目：条件比较成熟、任期内拟提请审议的法律草案”。2025年3月，《全国人民代表大会常务委员会工作报告》将修改网络安全法列入2025年的立法工作任务。修改工作启动以来，我办会同相关部门密切沟通，共同推进修改《网络安全法》工作，先后开展了调查研究、修正草案起草、征求中央和国家机关有关单位、面向社会公开征求意见等工作。在认真听取有关方面意见的基础上，形成了《网络安全法（修正草案再次征求意见稿）》。

二、修改思路

在《网络安全法（修正草案再次征求意见稿）》起草过程中，着重把握以下几点：一是坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平法治思想和习近平总书记关于网络强国的重要思想。二是坚持问题导向，重点强化网络安全法律责任，加大对违法行为处罚力度。三是坚持体系化衔接，加强与《数据安全法》《个人信息保护法》《行政处罚法》等相关法律有机衔接，在行政处罚的种类、范围、幅度等方面作出合理安排。四是坚持分类施策，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。

三、修改的主要内容

（一）关于网络运行安全的法律责任。结合实践中危害网络安全后果的情况，增加造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的和造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的情形，并参照《数据安全法》调整了现行《网络安全法》第五十九条罚款幅度，增加相应处罚规定；新增销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的法律责任；明确关键信息基础设施运营者使用未经安全审查或者安全审查未通过的网络产品或者服务行为的处置处罚措施。

（二）关于网络信息安全的法律责任。为防范新形势下网络信息内容安全风险对国家安全、政治安全带来的风险挑战，结合近年来网络信息内容执法实践，借鉴国外相关立法法律责任制度的新调整，完善现行《网络安全法》第六十八条、第六十九条针对的违法情形，调整未向有关主管部门报告和不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施情形的法律责任，明确对造成特别严重影响、特别严重后果的违法情形的处置处罚措施。

（三）关于个人信息和重要数据安全的法律责任。鉴于《数据安全法》《个人信息保护法》等有关法律、行政法规对现行《网络安全法》第六十四条第一款、第六十六条涉及的个人信息和重要数据违法行为的处罚作出了新的专门规定，明确转致适用的规定。

（四）关于从轻、减轻或者不予行政处罚的情形。统筹考虑《网络安全法》和《行政处罚法》的适用关系，专门新增一条衔接规定，明确网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果或者初次违法且危害后果轻微并及时改正等情形的，依法从轻、减轻或者不予处罚；明确有关主管部门依据职责制定相应的行政处罚裁量基准。

武汉市网络安全协会党支部召开组织生活会暨民主评议党员会议

2025年3月6日，武汉市网络安全协会党支部召开2025年度组织生活会暨民主评议党员会议，旨在深入贯彻习近平新时代中国特色社会主义思想，学习上级党组织各项文件精神，推动党建与协会业务深度融合，为武汉市网络安全事业发展注入强劲动力。会议由党支部书记刘悦恒主持，支部全体党员参加。

会前，党支部围绕**“深化学习、查摆问题、谈心谈话、整改落实”**四个关键环节，扎实开展筹备工作。在理论学习方面，组织党员深入学习总书记关于党的建设、党的自我革命的重要思想，以及考察湖北武汉重要讲话精神，集体研读党内法规，并结合理事会第五次会议精神，研讨细化年度工作要点，切实筑牢思想根基。同时，支部委员会和党员分别对照要求，全面查摆问题，形成“班子+个人”双清单；党支部委员之间、党员之间广泛开展谈心谈话，围绕行业发展深入交流，为会议顺利召开奠定坚实基础。

会议期间，党支部书记代表支部委员会作工作报告，详细通报问题查摆情况，并接受党员评议。全体党员围绕“政治素质、业务能力、服务意识、纪律作风”等方面，认真开展批评与自我批评，直言不讳地指出问题、提出建议，切实达到红脸出汗、相互促进的效果。随后，通过无记名投票的方式开展民主测评，客观公正地评价党员表现。

针对查摆出的问题，会议明确了“党建引领、问题导向、融合赋能”的整改方向，提出三项重点任务：**一是强化政治引领，**压实主体责任，严格落实“三会一课”、主题党日等制度，通过开展红色教育、联合党建等活动，推动学习贯彻习近平总书记关于网络强国重要思想走深走实；**二是聚焦工作落实，**对标协会相关会议部署，推进重点项目落实，确保工作任务落地见效；**三是支撑国家网安基地发展，**结合国家网安基地产业需求，着力赋能基地产业健康发展。

会议强调，要以此次组织生活会为新起点，把整改成效转化为推动网络安全事业发展的强大动力。持续提升政治站位，将上级党组织部署与我市网信工作紧密结合，依托协会各类平台资源，构建政产学研用融合生态，为城市现代化治理筑牢安全防线。

此次会议不仅是对党支部和党员的一次全面政治体检，更是推动协会发展的动员誓师。未来，武汉市网络安全协会党支部将以整改落实为重要抓手，为谱写中国式现代化武汉篇章贡献武汉网安力量。

党日活动丨武汉市网络安全协会联合多家单位开展党支部主题党日活动

联学共建聚合力　党建引领促发展

4 月 8 日，为深入贯彻中央关于加强社会组织党的建设工作的相关文件精神，深化党建与业务融合，武汉市网络安全协会党支部联合武汉云行政党支部、网安党支部、中金数谷科技有限公司党支部，于国家网安基地开展“联学共建聚合力，党建引领促发展”主题党日活动。活动以理论学习、实践研学、技术交流为主线，旨在通过跨领域协作激发基层党组织活力，为网络安全与数字经济发展注入红色动能。

活动期间，各支部党员代表立足岗位实际，围绕“以优良作风凝心聚力、干事创业”主题发表学习意见，强调通过作风建设强化责任担当，筑牢网络安全防线。会上，全体党员重温入党誓词，坚定理想信念，强化纪律意识。

活动注重党建与业务双向赋能。参会人员首先参观了黄鹤实验室，深入了解其在网络安全领域的技术突破与成果转化。中金数谷党支部分享超算中心在人工智能、大数据等领域的应用实践；黄鹤实验室团队通过专题汇报，展现党建引领下科技攻坚的生动案例。“实地观摩 + 技术共享”模式，推动了跨单位资源整合与协同创新，既强化了党员对行业前沿的认知，也推动了跨单位资源整合与协同创新。

在互动交流环节，各支部围绕党建与业务深度融合展开深入探讨。各支部书记一致表示，此次联学共

各党支部书记

参观黄鹤实验室

中金数谷党支部主讲人

黄鹤实验室团队主讲人

建活动，以“组织共建、资源共享、发展共促”为路径，为新时代党建引领行业发展提供了鲜活样本。

下一步，协会党支部将积极发挥网络安全专业性社会团体平台优势，推进社会组织党的组织和党的工作有效覆盖，创新党组织工作内容和活动方式，切实发挥好社会组织党组织的政治核心作用，为协会各成员党组织提供资源共享、合作共赢的交流平台，共同推动网络安全与人工智能、大数据等前沿技术深度融合组织建设，书写高质量发展新篇章。

武汉市网络安全协会
第二届第三次会长办公会成功召开

聚焦发展新征程　共绘网安新蓝图

——武汉市网络安全协会第二届第三次会长办公会成功召开

2025 年 1 月 21 日，武汉市网络安全协会第二届第三次会长办公会在武汉科技大厦协会会议室顺利召开。本次会议由协会会长潘宣辰主持，协会副会长、监事、秘书长、部分理事会员代表、部分协会工（专）委会负责人以及秘书处全体员工齐聚一堂，共商协会发展大计。

本次会议以习近平新时代中国特色社会主义思想和网络强国的重要思想为指引，集体学习了全国和湖北省网信办主任会议精神。会议强调，协会将坚定不移地协助各级网信主管部门守好网上阵地，坚决维护网络意识形态安全，加快构建大网络安全工作格局，为切实筑牢国家网络安全屏障贡献集体力量。

会议针对 2024 年协会工作进行了全面系统的回顾与总结，并起草了相关文件审议稿，围绕 2025 年的工作要点与计划安排、拟新增的内部管理制度、会员服务工作等重要议题展开了热烈讨论，进一步明确了协会未来的工作方向，相关成果将形成书面报告，提交至理事会议进行充分审议。本次会议还对召开协会第二届第五次理事会及第二届第四次会员大会的相关事宜进行了讨论和规划。

此次会议为协会 2025 年的工作指明了清晰方向，奠定了坚实基础。未来，在协会主管部门的坚强指导下，武汉市网络安全协会将持续团结广大会员单位，始终秉持积极创新、扎实工作的态度，不断提升网络安全保障能力与服务水平，全力为武汉市网络安全事业发展贡献更多力量，奋力守护网络安全防线，为城市数字化转型和高质量发展提供坚强有力的保障。

武汉市网络安全协会
第二届理事会第五次会议成功召开

武汉市网络安全协会第二届理事会第五次会议于 2025 年 2 月 27 日在协会新设立的会员活动中心顺利召开。本次会议在主管部门的指导下，全面总结协会 2024 年度工作成果，审议通过 2025 年工作计划及多项重要提案，为全市网络安全事业高质量发展凝聚共识、擘画蓝图。主管部门相关处室负责人到会指导，协会会长、副会长、监事、理事参会，各专（工）委会负责人、部分会员代表以及秘书处全体成员均列席参加。本次会议由协会秘书长刘悦恒主持。

会议审议并通过了《2024 年工作总结报告》《2024 年度财务情况报告》及《2025 年工作要点》。2025 年协会将不断深化会员服务，提升会员满意度；加强网络安全标准化建设，推动行业规范化发展；推广网络安全保险，构建数智安全金融保障机制；推动实战化人才培养，服务网络安全人才队伍建设；持续组织赛事活动，激发网络安全产业活力；加大网络安全宣传力度，提升公众网络安全意识；加强党建引领，推动协会内部治理与外部合作。

会长潘宣辰指出，协会新一年工作将继续在主管部门的指导支持下，扎实推进各项工作部署，进一步提高政治站位，紧密围绕国家网络安全战略布局，做好主管部门助手和参谋，强化行业协同联动，不断提升服务品质，切实为我市网络安全事业防风险筑屏障提供支撑保障。

会议还审议通过了各分支机构工作总结。会议一致认为，各分支机构工作务实推进，在各个领域取得了阶段性成效，为网络安全工作深入我市各个领域奠定了坚实基础。

武汉市网络安全协会会长潘宣辰

会议还充分发扬民主办会精神，就各理事、专家、会员以及秘书处提交的关于协会新增分支机构、专职员工人事管理制度、会员活动中心设立、本届理事会部分理事职务调整方案及新会员吸收方案等多项提案，进行了充分讨论和审议。各项提案论证充分材料详实，充分说明了大家对协会工作的关心和对协会服务水平不断提升的期盼，也为进一步夯实协会规范化办会路径提供了智力参考。

会议期间，协会会员活动中心正式揭牌，标志着协会服务能力建设迈上新台阶。据了解该活动中心将作为协会长期服务会员的场所，为广大会员提供交流合作、服务对接等活动平台。

会员活动中心揭牌

武汉人工智能研究院副院长彭骏作为特邀嘉宾发表专题分享，他深入阐释了人工智能与网络安全融合发展的新趋势。他提出，要构建“AI+ 网络安全”协同创新机制，通过算法优化不断提升大模型网络攻击监测预警能力。会议同时吸纳了多项行业建设性意见，武汉市中心医院信息中心主任李海对医疗行业网络安全及数据安全提出了相关建议，呼吁共同努力不断提升医疗领域网络安全防护能力水平，搭建多方协同、技管并重的立体防护体系。

会议强调，武汉市网络安全协会要在主管部门的有力指导和支持下，不断凝聚团结广大理事会员，助力国家网安基地建设，加快产业进步和技术创新，筑牢网络安全屏障，推动信息赋能城市发展，支撑全市网信事业高质量发展强根基聚合力，为全市加快建成中部地区崛起重要战略支点中当好龙头、走在前列，做出“武汉网络安全”集体贡献。

会议最后审议通过了《关于召开协会第二届第四次会员大会的提案》并为新当选的理事会成员和新会员举行了授牌仪式。

特邀嘉宾 武汉人工智能研究院副院长彭骏

特邀嘉宾 武汉市中心医院信息中心主任李海

武汉市网络安全协会第二届理事会第五次会议新晋会员单位名单

副会长单位

奇安信安全技术（武汉）有限公司

中国电信股份有限公司武汉分公司

理事单位

武汉市德发电子信息有限责任公司

武汉观安信息技术有限公司

会员单位

武汉粟泰信息科技有限公司

北京网御星云信息技术有限公司

武汉中昊空间科技有限公司

武汉华夏理工学院

小米科技有限责任公司

武汉攀升鼎承科技有限公司

此排名不分先后

武汉市网络安全协会会员活动中心正式落户江岸区三阳路 88 号三阳中心 B 座 20 层，该中心紧邻汉口江滩交通便利，作为网安产业资源聚合地，将打造我市网络安全行业 " 赋能站 "，为会员单位提供技术交流、政策咨询、项目孵化和生态协同的全链条服务。

武汉城市职业学院到访武汉市网络安全协会共商产教融合合作

2025 年 3 月 14 日，武汉城市职业学院计算机学院副院长王世刚一行到访武汉市网络安全协会，双方围绕产教协同、人才培养等议题展开交流。武汉市网络安全协会秘书长刘悦恒及相关负责人参与座谈。

会上，王院长提出联合打造“产教融合共同体”的规划，旨在通过校企联动推动教育链与产业链深度融合，将依托协会资源，优化课程体系并强化学生实践能力。同时表达了加入协会的意愿，以进一步深化与网安行业企业合作。

刘秘书长对合作提议表示支持，并强调将整合行业资源，推动人才培养与产业需求精准对接。双方还就网络安全技术趋势、行业发展方向等交换意见，未来计划在技术研发、标准制定等领域加强协同创新。

此次座谈为校协合作奠定基础，双方将以产教融合为抓手，共同为网络安全产业提供人才与技术支持，助力武汉市建设高水平网络安全生态。

武汉城市职业学院计算机学院教学办公室副主任叶飞、网络教研室专任教师付强、教学办公室周珣；武汉市网络安全协会办公室主任张玉萍、政府服务和科研部主任乔奇、宣传专员何溪山参加会议。

武网安协赴中金数据武汉超算开展会员单位走访调研

为落实协会第二届理事会第五次会议部署，进一步加强会员单位服务保障工作，3 月 25 日，武汉市网络安全协会秘书长刘悦恒率秘书处一行赴会员单位中金数据（武汉）超算技术有限公司开展走访调研。协会相关部门负责人参加调研。

在中金数据武汉超算，协会一行受到公司总经理艾微的热情接待。艾微总经理详细介绍了企业发展历程及核心业务布局，重点阐述了公司在高性能计算、大数据处理、人工智能等领域取得的技术突破。作为国家高新技术企业和湖北省专精特新＂小巨人＂企业，中金数据武汉超算自主研发的超算解决方案已成功应用于智慧城市、生物医药、智能制造等多个领域，其技术实力和行业影响力获得同行业高度认可。

座谈会上，刘秘书长代表协会对中金数据武汉超算正式加入协会表示热烈欢迎。他指出，当前正值武汉在“加快建成中部地区崛起重要战略支点中当好龙头、走在前列＂的关键时期，协会将紧紧围绕全市网信工作重点，在主管部门的指导下，团结广大会员，重点推进全市关键信息基础设施保护、数据安全治理、网络安全人才培养等工作。希望中金数据武汉超算充分发挥超算技术优势和数据中心基础设施优势，积极参与协会各项活动，共同探索＂网安 + 超算＂融合发展新模式。

随后，协会人才服务部负责人严媛就专业技术人才职称评定等政策进行了详细解读，会员服务部负责人张玉萍重点介绍了协会年度重点活动安排。双方就建立常态化沟通机制、联合开展技术合作等事项达成初步合作意向。

调研期间，刘悦恒秘书长代表协会向中金数据武汉超算授予＂会员单位＂牌匾。艾微总经理表示，公司将以此次加入协会为契机，进一步加强与协会各会员单位的技术交流与资源共享，为武汉网络安全产业高质量发展贡献力量。

中金数据武汉超算网安服务部王俊华、市场部李亚妨，协会宣传部何溪山、基地服务办周怡等陪同调研。武汉市网络安全协会将持续深化会员服务体系建设，通过走访调研、专题培训、供需对接、实战演练、推介宣传等多种形式，助力会员单位创新发展，为武汉建设国家网络安全人才与创新基地提供有力支撑。

《安安说网安之科普小讲堂》第一期正式上线

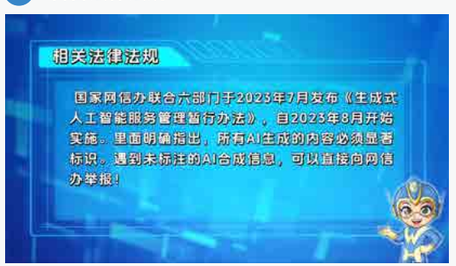
武汉市网络安全协会制作的《安安说网安之科普小讲堂》第一期正式上线啦！今天探索 AI 换脸真相，赶快来和安安一同揭秘吧！

本期主要内容

01 典型案例报道

近期 AI 人工智能风靡网络，但也带来相应的网络安全风险。央视报道一起 AI 换脸诈骗事件给 AI 网络安全敲响警钟。

02 科普法律法规



国家网信办联合六部门发布的《生成式人工智能服务管理暂行办法》

03 传授相关技巧

安安分享识别 AI 换脸诈骗视频技巧

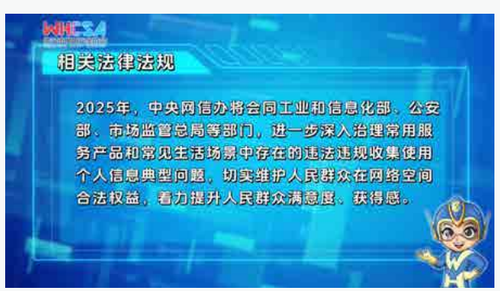
《安安说网安之科普小讲堂》第二期个人隐私保护需警惕

本期主要内容

01 典型案例报道

央视报道“网络养盒”事件

02 科普法律法规



中央网信办会同三部门开展专项行动

03 03 传授相关技巧

安安分享个人信息保护办法

武网安协第五期会员交流互访活动

——走进武汉德发电子

全民国家安全教育日

为深入贯彻总体国家安全观，促进会员单位之间的交流沟通与合作，推动网络安全技术人才职称申报工作的顺利开展，武汉市网络安全协会于 2025 年 4 月 15 日举办了第五期会员交流互访活动。

本次活动以“凝心聚力共促发展，团结合作共保网安”为主题，走进了新晋理事单位武汉市德发电子信息有限责任公司，吸引了网络安全协会会员单位积极参与。活动得到了会员单位武汉学院、湖北珞格科技发展有限公司、湖北天融信网络安全技术有限公司、武汉鼎安华盛科技有限公司、武汉安域信息安全技术有限公司、绿盟科技集团股份有限公司武汉分公司、武汉安恒信息科技有限公司的大力支持。

活动伊始，与会人员参观了德发公司的企业文化墙，深入了解企业的发展历程和文化内涵。随后，德发公司副总裁程俊致欢迎词，表达了对与会嘉宾的热烈欢迎。德发公司 IT 服务售前工程师程梦娇分享了德发安全运营服务的特色与优势，在日常工作中如何做

好客户与德发自身的安全运营工作，保障业务的连续开展。

在学习环节，与会人员共同观看了 415 全民国家安全教育日公开课视频，结合习近平总书记关于网络安全的重要论述，围绕国家安全与网络安全的关系进行了深入学习。

德发公司副总裁程俊

德发公司代表程伟分享了企业在网络安全领域的实践经验，进一步增强了与会人员对网络安全重要性的认识。

德发公司代表程伟

互动交流环节中，与会人员围绕国家安全理念、信息安全保障以及企业网安实践等话题展开了热烈讨论，分享了各自的工作经验和见解。

武汉市网络安全协会人才服务部负责人严媛详细解读了网络安全技术人才职称申报工作的注意事项，严主任的讲解深入浅出，为与会人员提供了清晰的指导方向。

武汉市网络安全协会人才服务部负责人严媛

武汉市网络安全协会党支部书记、秘书长刘悦恒做了总结发言，讲述了协会作为桥梁纽带，积极服务会员单位促进网络安全人才发展的初心和相关人才职称申报的推进工作，鼓励各会员单位相互走访取长补短，共同维护好国家安全和网络安全，国家安全与网络安全息息相关，希望通过此类活动，进一步增强行业责任感，推动网络安全技术人才队伍建设，为维护国家安全贡献力量。

武汉市网络安全协会党支部书记、秘书长刘悦恒

活动最后，各会员单位参会代表人员依次发表了对此次活动的感受，并表达对网络安全事业的期望。

本次交流互访活动不仅加深了会员单位之间的了解与合作，也为网络安全技术人才职称申报工作提供了有力支持。未来，武汉市网络安全协会将持续践行协会责任，为会员提供更多交流互动的平台，为网络安全事业注入持久动能。

武汉市网络安全协会联合多方开展国家安全教育日主题活动

为落实总体国家安全观，使国家安全教育意识深入民心，增强大众的国家安全法治观念。4 月 16 日，武汉市网络安全协会联合湖北艺术职业学院和我会副会长单位武汉安域信息安全技术有限公司，于国家网络安全人才与创新基地开展国家安全日的宣传教育活动。

活动伊始，湖北艺术职业学院的师生们参观了网络安全学习长廊、密码科技展厅及工业安全靶场三大教学场景。通过动态影像呈现我国网络安全发展历程，

并运用虚拟现实技术模拟电力系统攻防场景。

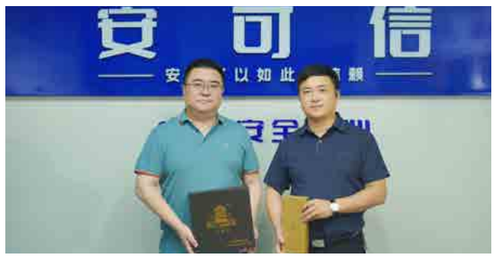
学习环节，武汉市网络安全协会秘书长刘悦恒为湖北艺术职业学院的学生们进行《国家安全日·网络安全“艺”起守护》专题授课，将网络安全与艺术创作深度融合。“同学们，想象一下：明天就是全国舞蹈大赛总决赛，你们精心编排 3 个月的原创作品，突然在直播平台上被替换成诡异的黑屏画面；或者比赛前，指导老师手机收到伪装成组委会的钓鱼链接，点开后训练视频全被加密 … 这些不是编舞剧情，而是可能发生的网络安全事件！今天，我们就为你们的舞蹈梦想穿上‘数字防护服’！”

从数字艺术作品确权难题出发，剖析社交媒体时代艺术工作者面临的隐私泄露风险，传授口令设置等防护技巧。" 艺术是时代的镜像，网络安全则是镜像的守护者。" 刘悦恒的结语引发热烈掌声。学生们在课后分享环节表示“以前觉得网络安全离自己很远，通过这次研学才发现它与生活息息相关”、" 艺术创作需要舞台安全，网络空间更需要系统安全。”

本次国家安全主题宣传教育活动的开展，不仅增强了湖北艺术职业学院师生对国家安全问题的认识和理解，提升了法治素养，更进一步促进师生树牢总体国家安全观，增强了国家安全的责任感、使命感和行动自觉。未来武汉市网络安全协会将持续发挥行业枢纽和专业性社团作用，为网络强国建设筑牢数字安全基石。

武汉市网络安全协会赴重庆开展交流并签署战略合作协议

4 月 21 日，武汉市网络安全协会率三家会员代表赴重庆开展交流活动并签订战略合作协议。我会先后访问重庆市大数据和人工智能产业协会、重庆安可信科技发展有限公司、中国通信服务重庆公司、重庆市中冉数字科技有限公司等网络安全、大数据和人工智能相关企业并开展座谈，深入探讨两地产业协同发展路径。









在渝期间，我会受邀出席“赋能数据要素 X 医疗健康合规发展暨渝鄂网络空间安全交流沙龙”，本次沙龙汇聚重庆行业协会、医疗机构、科技企业及法律界代表百余人，围绕数据合规、网络安全、智慧医疗创新等议题展开深入探讨。重庆市互联网界联合会主席王茵，重庆市卫生健康统计信息中心主任石任重、重庆市大数据和人工智能产业协会副理事长陈宏，重庆市卫生健康信息学会秘书长肖兵，重庆市律师协会数字经济专委会主任罗治波等领导出席了本次沙龙。

聚焦数据安全与合规
共筑医疗健康数字防线

活动伊始，重庆市大数据和人工智能产业协会副理事长陈宏领学了习近平总书记在近期关于数字经济与医疗卫生事业的重要讲话并致欢迎辞，强调数据要素在医疗健康领域的战略价值，呼吁各方协同构建安全、可信的数据流通生态。

重庆市律师协会数字经济专委会主任罗治波在致辞中指出，法律与技术双重护航是医疗数据资产化关键，需以合规为基石激活数据价值。


聚焦合规与安全
筑牢数据治理基石

重庆市律协数字经济专委会副主任朱杰在《数据要素 X 医疗健康领域数据资产化合规风险及应对》演讲中，系统剖析了医疗数据确权、流转中的法律难点，并提出“法律 + 技术”双轮驱动的合规框架。

随后，重庆安可信科技发展有限公司董事长沈致柯以《践行网络强国战略，守护健康中国生命线》为题，展示了 DeepSeek 智能化工具在医疗数据分类分级、隐私计算中的实践成效，强调技术赋能安全治理现代化


的必要性。

杭州帕拉迪网络科技有限公司市场李亚楠则从技术创新角度，提出构建“智能防御”新范式，通过动态加密与威胁感知技术实现医疗数据的全生命周期防护。

数字化路径与实践
释放数据要素价值

重庆市信息通信咨询设计院院长张晓琴在《健康重庆的数字化建设路径》中，提出“云网端”协同、全域联动的区域医疗数字化转型方案。国信中健数字科技重庆公司总经理李剑星则从投资视角，分享了可信流通数据空间的建设蓝图，强调多方共治与市场化运营机制。

重庆若可网络安全测评工程师何倩结合测评实践，指出医院数据保护需重点关注权限管理、日志审计与应急响应三大环节。广电计量重庆公司总监冉清华进一步强调数据质量对价值挖掘的核心意义，提出通过标准化清洗与跨域校验提升医疗数据可用性。

技术创新与生态构建
探索未来医疗新范式

苏州国本董事长曹岭展示了多模态 AI 大模型在医院私有化部署的实践案例，展示其在辅助诊断等方面的应用成果，为智慧医疗发展提供新技术路径。西部提尔技术总监盛春则创新性提出液冷式智算中心方案，以绿色节能技术支撑医院高密度算力需求。

中冉科技张秀秀聚焦智能医疗数据共享平台建设，呼吁打破“数据孤岛”，驱动医疗产业要素化升级。

武汉市网络安全协会秘书长刘悦恒在会上重点介绍了武汉市网络安全协会概况同时展示了国家网络安全人才与创新基地的建设情况，并与重庆市大数据和人工智能产业协会签订战略合作协议。

根据协议，双方将成立联合工作组，共建信息共享平台，推动两地企业加强合作、促进数据共享利用，协同推进产业链上下游发展。交流会上，刘悦恒秘书长邀请重庆企业赴武汉展业，为企业在汉发展提供支持和服务。

此次交流进一步深化了渝汉两地网络安全产业协作共识。双方将以国家网安基地为纽带，推动资源共享与技术互通，共同构建数字安全生态。

武汉市网络安全协会两大分支机构筹备工作全面推进

近日，武汉市网络安全协会根据第二届理事会第五次会议精神，秘书处统筹推进医疗卫生与健康分会、人工智能安全专业委员会两大分支机构筹备工作，聚焦重点领域网络安全治理体系建设，为城市数字化转型筑牢安全底座。

医疗卫生与健康分会筹备工作会在协会会议室召开。会议围绕组织制度建设作出相关部署。会议认为，分会将以提升医疗卫生与健康行业网络安全防护能力为核心目标，推动医疗数据安全管理、医疗信息系统安全应用，完善医疗行业网络安全风险管理体系，促进医疗信息技术与网络安全融合发展。分会将搭建＂互联网＋安全＋医疗健康＂协同平台、制定相关团体标准规范、开展风险评估、提供培训服务、推动技术创新、促进产学研合作等，筑牢我市医疗卫生和健康领域网络安全屏障。

人工智能安全专委会筹备工作会在武汉人工智能研究院召开。随着大模型应用、人形机器人量产、智能体场景化落地等技术的加速渗透，人工智能产业面临的安全挑战日益凸显。筹备会议审议了相关筹备工作文件，听取了各参会单位的相关建议，一致认为，该

机构将在技术研发与创新、公共服务平台搭建和规范标准制定、应用场景拓展、促进人工智能安全人才培养和产业集聚等方面开展工作。依托武汉国家新一代人工智能创新发展试验区和网络安全人才与创新基地＂双区＂优势，专委会着力构建全链条服务体系，推动我市人工智能产业安全健康快速发展。

目前，两大分支机构已完成工作条例、年度计划等文件起草，负责人选聘工作有序推进。随着医疗卫生、人工智能等重点领域安全治理体系的完善，协会正以＂技术创新与安全合规双轮驱动＂模式，加速构建覆盖全域的网络安全生态，为护航武汉社会经济高质量发展注入新动能。

武汉市网络安全协会第二届理事会第六次会议成功召开

2025 年 5 月 16 日下午，武汉市网络安全协会通过视频会议召开第二届理事会第六次会议。协会领导班子成员、全体理事、监事、分支机构负责人、特邀代表及秘书处工作人员等参与会议。本次会议聚焦行业发展关键议题，完成多项重要决议，标志着协会在规范化治理与产业协同发展上迈出关键步伐。

一、会费改革·地址焕新：治理再升级会议集体研究了《关于协会个人会员会费标准调整的提案》，为响应国家减轻企业和从业人员负担号召，不断扩大协会覆盖面，优化服务效率和质量，协会个人会员会费标准拟进行大幅度下调。同时会议研究了《关于协会注册地址变更的提案》，两项提案理事会予以全票同意，按照协会章程有关规定，上述两项提案报下次会员大会决议。

二、分支落地·领域深耕：安全再进阶本次会议重点完成了三大分支机构的组建工作，为武汉网络安全事业注入新动能。根据相关提案：

协会医疗卫生与健康分会将聚焦医疗卫生行业网络安全，推动医疗数据安全管理、信息系统安全应用，制定行业标准、组织风险评估与培训、促进产学研合作。分会接受市委网信办网安处和市卫生健康信息中心共同指导，会议选举武汉市中心医院为会长单位，武汉市中医院为秘书长单位，奇安信科技集团股份有限公司为执行秘书长单位。

协会人工智能专业委员会旨在促进人工智能＋安全产业融合，助力武汉打造 AI 安全创新集聚区，带领成员单位开展技术研发攻关、标准体系建设、应用场景拓展、人才培养等工作。专委会接受市委网信办、市经信和科创部门的共同指导。会议选举武汉人工智能研究院为主任单位武汉网络安全技术有限公司（黄鹤实验室）为秘书长单位，武汉鼎安华盛科技有限公司为副秘书长单位。

近日，协会受国家网安基地建设办公室的委托，承担了国家网安基地产业联盟组建运营等重要工作，会议决定成立协会国家网络安全人才与创新基地产业联盟工作委员会承担相关工作任务，会议同意全体理事会成员取得工委会委员资格，建议全体会员同时取得联盟成员资格，相关工作条例及委员建议名单获通过，同意联通湖北公司代表联通武汉公司参与联盟具体工作。联盟工委会的成功组建标志着协会在支撑国家网安基地产业发展方面提供了坚实的制度和组织保障。

三、新员加盟·提案推动：动能再汇聚会议还审议通过了中金数据（武汉）超算技术有限公司、武汉城市职业学院、湖南省金盾信息安全等级保护评估中心有限公司、武汉鼎安华盛科技有限公司、浪潮智慧科技（武汉）有限公司 5 家单位入会申请，各新会员的加入将为协会 不断注入新的活力。

此外，安恒信息提出的《关于构建“综合安全防护平台”（城市盾、行业盾）的建议》提案获通过，秘书处将跟进办理。新当选的医疗卫生健康分会会长、武汉市中心医院信息中心主任李海，人工智能专委会秘书长、武汉网安公司黄鹤实验室总经理杨志刚先后发言，分别表态将带领各分支机构为武汉网络安全工作贡献新的力量。当前，武汉正加速建设国家网安基地，武汉网安协会作为全市网络安全行业的枢纽，使命光荣责任重大。本次会议以“规范治理、高效协同”为原则，在会员服务、组织架构、产业协同等方面取得重要进展。协会将以本次会议为新起点，凝聚行业共识，落实决议事项，提升服务效能，推动武汉网络安全事业迈向新台阶，为全市各领域数智化转型和建设保驾护航。

我会代表国家网安基地产业联盟出席世界数字教育大会并在平行会议参加圆桌讨论

2025 年 5 月 15 日，世界数字教育大会平行会议“数字教育安全与伦理：挑战、共识与行动”在武汉国际会议中心隆重举行。本次会议由教育部学校规划建设发展中心指导，武汉市教育局、武汉网络安全大学筹建办、武汉软件工程职业学院承办，聚焦全球教育数字化转型中的安全与伦理议题。武汉市网络安全协会代表国家网络安全人才与创新基地产业联盟（以下简称“联盟”）参与会议，联盟秘书长、武汉市网络安全协会秘书长、高级工程师刘悦恒受邀在“数字教育安全与伦理：挑战、共识与行动”平行会议中圆桌讨论环节发言。

01 会议盛况：大咖云集共商数字教育安全

武汉市人民政府市长盛阅春、教育部副部长王光彦、世界互联网大会国际组织秘书长任贤良等领导出席会议并致辞，图灵奖得主约翰·霍普克洛夫特、诺贝尔物理学奖得主巴里·巴里什等国际权威专家发表主旨报告，围绕数字教育安全的技术前沿与伦理构建展开深度探讨。会议期间，“人机交互与信息安全中心”正式揭牌，《安全人工智能赋能产教融合创新联合行动计划》重磅发布，为数字教育安全领域的产教融合注入新动能。

02 圆桌讨论：聚焦产教融合的“武汉方案”

在“AI 赋能人才培养、产教融合的创新实践与安全挑战”圆桌讨论环节，各高校校长和专家发表了专业见解，刘悦恒秘书长作为产业界代表，结合国家网安基地的实践经验，从三个层面分享了对数字教育安全与伦理的思考。

（一）国家网安基地：打造产教融合“武汉样本”

作为 2016 年落地武汉的全国首个国家网安基地，目前已形成“人才、创新、产业”三位一体发展格局：两百余家网安企业及各类研发科研创新平台集聚，构建起“芯片安全—数据安全”全产业链生态；首创“马路对面的产学研”模式，武大、华科网安学院与企业一街之隔，实现“上午课堂理论、下午企业实战”的沉浸式培养，全国唯一网安公立大学——武汉网络安全大学筹建加速，未来将成为高端网安人才的“蓄水池”。

（二）产教融合：破解安全伦理难题的关键路径

针对 AI 教育应用中的算法偏见、数据隐私等挑战，刘悦恒指出，国家网安基地的实践证明，深度产教融合是实现技术攻坚、标准构建、人才储备协同突破的核心路径。例如高校可依托产业优势制定技术标准，为教育智能化转型提供“安全指南”，“网络安全万人培训计划”则聚焦培养“技术 + 伦理”复合型人才，从人才源头筑牢安全防线。

（三）三点倡议：构建产教融合“ 安全共同体”

结合湖北“51020”现代产业集群和武汉“965”产业链布局，刘悦恒代表联盟和协会提出三点倡议：一是筑牢经济产业数字化安全基座，聚焦芯屏端网、新能源汽车等重点产业，打造“政产学研用”一体化安全平台，攻关车联网数据安全、工控安全等关键技术；二是深化“网安 +X”融合培养，推动网安学科与 AI、大数据等专业交叉，共建现代产业学院，推行“课程对接产业标准、实训贴近真实场景”的培养机制；三是强化标准与技术输出，联合高校制定教育 AI 算法透明、产教数据共享安全等紧缺标准，加速成果转化，形成“武汉标准引领、基地辐射全国”的数字化安全解决方案生态。

03 展望未来：携手构建安全共同体

此次会议为全球数字教育安全与伦理治理提供了交流平台，国家网安基地的“武汉实践”获得与会专家高度认可。武汉市网络安全协会将继续助力国家网安基地产业联盟运转，以产教融合为纽带，凝聚高校、企业、社会多方力量，共同构建“安全有保障、创新有活力、人才有支撑”的产教融合共同体，为武汉数字经济高质量发展和全球教育数字化转型贡献“武汉力量”。

二项网络安全国家标准获批发布

根据 2025 年 2 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2025 年第 4 号），全国网络安全标准化技术委员会归口的 2 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	代替标准号	实施日期
1	GB/T 19713-2025	网络安全技术 公钥基础设施 在线证书状态协议	GB/T 19713-2005	2025-09-01
2	GB/T 37027-2025	网络安全技术 网络攻击和网络攻击事件判定准则	GB/T 37027-2018	2025-09-01

六项网络安全国家标准获批发布

根据 2025 年 3 月 28 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2025 年第 6 号），全国网络安全标准化技术委员会归口的 6 项国家标准正式发布。具体清单如下：

序号	标准编号	标准名称	实施日期
1	GB/T 45409-2025	网络安全技术 运维安全管理产品技术规范	2025-10-01
2	GB/T 45389-2025	数据安全技术 数据安全评估机构能力要求	2025-10-01
3	GB/T 45392-2025	数据安全技术 基于个人信息的自动化决策安全要求	2025-10-01
4	GB/T 45396-2025	数据安全技术 政务数据处理安全要求	2025-10-01
5	GB/T 45404-2025	数据安全技术 大型互联网企业内设个人信息保护监督机构要求	2025-10-01
6	GB/T 45406-2025	网络关键设备安全技术要求 可编程逻辑控制器（PLC）	2025-10-01

武网安协发布五项团体标准

各分支机构，各单位会员，各有关单位：

依照《武汉市网络安全协会团体标准管理办法（试行）》，批准发布下列团体标准，现予公告。

序号	标准编号	标准名称	制、修订	实施日期
1	T/WHCSA 003—2024	制造业数据安全管理中的数据分类分级方法指南	制订	2025 年1月1日
2	T/WHCSA 004—2024	智慧园区网络安全防御体系建设指南	制订	2025 年1月1日
3	T/WHCSA 005—2024	网络安全人才实战化训练环境建设规范	制订	2025 年1月1日
4	T/WHCSA 006—2024	数据要素场内流通安全评估规范	制订	2025 年1月1日
5	T/WHCSA 007—2024	网络安全风险量化评估规范	制订	2025 年1月10日

武网安协联合中国网络空间安全协会发布《智能网联汽车网络安全检测技术要求》团体标准

各相关单位：

根据《中国网络空间安全协会团体标准管理办法（试行）》以及《武汉市网络安全协会团体标准管理办法（试行）》的相关规定，经评审组专家审查通过，中国网络空间安全协会及武汉市网络安全协会组织批准《智能网联汽车网络安全检测技术要求》(T/CSAC 019-2025/T/WHCSA 008-2025) 团体标准，现予以联合发布，自 2025 年 8 月 22 日起实施。

该标准起草单位：湖北天融信网络安全技术有限公司、国家计算机网络应急技术处理协调中心、国家计算机网络应急技术处理协调中心湖北分中心、武汉市公安局交通管理局、东风汽车集团有限公司研 发总院、岚图汽车科技有限公司、东风悦享科技有限公司、东风商用车有限公司、襄阳达安汽车检测中 心有限公司、中机寰宇认证检验股份有限公司、东风汽车集团股份有限公司猛士汽车科技公司、中移（上 海）信息通信科技有限公司、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、湖北大学网络空间安全学院、华中师范大学、湖北汽车工业学院，湖北省电子信息产品质量监督 检验院、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、广电计量检测（武汉）有限公司、宝牧科技（天津）有限公司武汉分公司。

该标准主要起草人：孙秉稷、范雪俭、左世涛、吕露、安高峰、胡雨翠、蔡倩楠、曹岚、李中戈、刘悦恒、乔奇、张玉萍、严媛、蒋凌云、张绳武、刘青、黄传明、付琳、陈翔、孙伟、陶先锋、刘翀、代薇、李宏伟、田明明、黄鑫、林凯、韩鹏、左少雄、翟亦康、牟飞、于乐、马禹昇、赵威、付超、曹 越、庄园、胡胜山、向剑文、何鹏、潘俊杉、陈嘉耕、陈宇峰、徐煦、柳少凯、李永龙、张海春、唐迪、肖海涛、张瑶

第二届武汉网络安全创新论坛开幕

4 月 23 日第二届武汉网络安全创新论坛在国家网络安全人才与创新基地（下称“网安基地”）启幕

来自全国网络安全领域的政、产、学、研各界精英，齐聚武汉临空港经开区（东西湖区），聚焦网络安全技术与产业深度融合，发布多项重磅成果，为网络安全能力建设注入新动能。

此图来源：东西湖融媒体中心

作为网络安全领域的年度盛会，本届论坛以“融合 • 创新 • 突破”为主题，设置了 1 场主论坛，6 场分论坛及 15 项重点活动，内容涵盖政策解读、技术交流，成果展示、产学研对接等。

主论坛上，三位顶尖网络安全专家分别作主旨报告，从密码技术、协同防御到网络架构，层层递进勾勒出网络安全的中国方案，更解读武汉作为国家网络安全高地肩负的时代使命。

国家网安基地产业投资基金签约举行

该基金是武汉产业投资控股集团和东西湖区市区两级联动组建，总规模 30 亿元，一期 5 亿元，将为国家网安基地发展注入强劲动能。

国家网安基地产业项目签约举行

武汉临空港经开区与上海三零卫士信息安全有限公司、启明星辰信息技术集团股份有限公司、浙江瑞基控股有限公司、众数信息科技有限公司、武汉虹安信息有限公司签约，将在数据安全、人工智能安全等领域展开合作。

主论坛发布了 2024 年度十大优秀网络安全创新成果，为 2024 网络产品安全能力提升计划优秀单位及个人、网络安全学院学生创新资助计划一期优秀学生及指导老师颁奖，并启动 2025 网络产品安全能力提升计划、第三期网络安全学院学生创新资助计划及 2025 网络安全大讲堂三个项目，构建技术研发、人才储备与社会教育协同发展的生态体系。

武汉市委网信办、武汉临空港经开区管委会、中国联通武汉市分公司三方签约，将进一步融合优势、整合资源、共谋长远发展。

本届论坛持续两天，中央、省、市网信部门领导，网络安全专家学者，华为、腾讯、蚂蚁集团、天融信等头部网络安全企业代表，将针对人工智能安全、智能网联安全、云安全、开源软件安全、关键信息基础设施保护、个人信息保护、网信企业社会责任等热点领域展开专题研讨。

截至今年，网安基地一期 4 平方公里核心区建成，注册企业超 300 家，培育规上企业 28 家、“瞪羚企业”8 家、上市企业 2 家，核心区营收产值规模突破 50 亿元，“1+2+N”特色产业体系逐渐形成。目前，武汉临空港经开区正规划打造 60 平方公里的网安科技新城，布局“一核三园四区”，建设产城融合的“中国网谷”。

本次论坛活动由武汉市人民政府主办，中国网络空间安全协会、武汉临空港经开区管委会承办，武汉市网络安全协会参与了筹备工作。

网络安全创新企业家座谈会在武汉召开

近日，网络安全创新企业家座谈会在第二届武汉网络安全创新论坛期间举办，会议由中央网信办副主任、国家网信办副主任王京涛主持。

王京涛指出，当前网络安全产业要加大从“合规驱动”向“风险驱动”转变的力度，通过政产学研用深度融合，构建弹性化、实战化的安全生态。鼓励企业秉承网络空间命运共同体的理念，积极拓展海外市场，同时通过海外实践反哺国内技术创新，凝聚合力，共建技术共研、标准互认、信息共享的协同机制。

会上，华为、天融信、安恒信息、奇安信、拼多多、腾讯公司、360、蚂蚁集团、恒安嘉新、深信服、中兴通讯等多家企业负责人，聚焦关键信息基础设施保护、人工智能安全治理、数据安全和个人信息保护、网安人才培养等领域，就推动网络安全产业高质量发展建言献策。

中央网信办有关司局负责同志以及 40 多家企业代表参会。

第二届武汉网络安全创新论坛
——关键信息基础设施安全保护分论坛在武汉召开

4 月 24 日，由中国网络空间安全协会关键信息基础设施安全保护专委会主办，中国互联网发展基金会支持的第二届武汉网络安全创新论坛—关键信息基础设施安全保护分论坛在武汉召开。中央网信办网络安全协调局有关负责同志出席会议并致辞

本次分论坛以“高质量构建关基安全保障体系”为题，深入探讨关键信息基础设施安全保护的新思想、新方法、新技术、新举措。军事科学院系统工程研究院研究员尹浩，北京交通大学教授、移动专用网络国家工程研究中心主任张宏科，中国网络空间安全协会副理事长、关基专委会主任委员孟丹作主旨报告。中国工商银行首席技术官吕仲涛等来自通信、能源、交通、金融、电子政务等重要行业领域和网信企业的技术专家在会上做专题报告。中国网络空间安全协会副秘书长、关基专委会秘书长杜阿宁作关基专委会年度重点工作计划介绍，并宣布根据成员单位呼吁将重要行业领域案例征集申报截止时间延期至 5 月 15 日。

与会代表普遍表示，本次论坛聚焦重要行业领域信息基础设施安全框架、解决方案与实践案例，具有鲜明的技术专业性和实践指导性。希望关基专委会建立常态化交流机制，通过定期举办行业细分领域研讨，持续输出经过实战验证的最佳实践方案，为全国重要行业领域单位提供参考。

来自全国重要行业领域单位、高校、研究机构以及相关地方网信主管部门的 200 余名代表参会。

关键信息基础设施安全保护分论坛议程分享

报告题目	报告嘉宾
第一阶段 战略启航·共筑数智未来 主持人：谢晓辉 关基专委会副主任委员、中国海油集团有限公司信息技术中心执行副主任	
致辞	中央网信办网络安全协调局有关负责同志
主旨报告	尹浩 军事科学院系统工程研究院研究员
	张宏科 北京交通大学教授、移动专用网络国家工程研究中心主任
	孟丹 中国网络空间安全协会副理事长、关基专委会主任委员
关基专委会年度重点工作计划介绍	杜阿宁 中国网络空间安全协会副秘书长、关基专委会秘书长
工商银行关键信息基础设施安全保护实践	吕仲涛 中国工商银行首席技术官
中国华电关键信息基础设施安全保护——看管监控数字化安全保障体系研究与设计	罗建东 关基专委会专家、中国华电集团有限公司数智中心副主任
面向民航关基的网络安全保障体系	顾兆军 中国民航大学教授
通信领域关基设施网络安全保护体系与实践	谢攀 中国联通网络与信息安全部副总经理
第二阶段 科技护航·安全赋能发展 主持人：郭峰 关基专委会副主任委员	
电力监控系统安全防护的回顾及关保工作的思考	胡红升 关基专委会专家、国家能源局信息中心原副主任
新形势下关基保护的新思维和新方法	吴云坤 关基专委会副主任委员，中国电子集团首席科学家、科技委副主任，奇安信集团总裁
网络安全ERP(SecERP)助力中国海油关键信息基础设施保护数字化转型	王英梅 关基专委会专家、中国海洋石油集团有限公司信息技术中心监控运营室主任
AI时代下的关基挑战	张福 青藤云安全创始人
金融基础设施数据安全治理体系建设探索与实践	张爽 关基专委会专家、中央国债登记结算有限责任公司信息科技部副主任
国产算力支撑关基安全的思考与实践	龚颜 华为鲲鹏生态部副部长
机制化构建数字政府关基防护体系——广东省政务云安全保护实践经验	罗奇伟 关基专委会专家、广东省政务服务和数据管理局安全管理处处长
长期共性网安问题根源分析——实战专家经验模型助力关基保护	郭峰 关基专委会副主任委员、中国电子科技集团有限公司安全专家

人工智能生成合成内容标识政策法规宣讲会在武汉举办

为积极推动《人工智能生成合成内容标识办法》（简称《标识办法》）及 GB 45438-2025《网络安全技术 人工智能生成合成内容标识方法》（简称《标识方法》）的落地实施，切实提升内容安全治理的能力，4 月 24 日，“人工智能生成合成内容标识政策法规宣讲会（湖北站）”在武汉举办。

本次宣讲会由中央网信办网络管理技术局、湖北省委网信办指导，中国网络空间安全协会人工智能安全治理专委会主办。多位长期在人工智能治理、标准制定和法律政策研究领域深耕的专家围绕标识法规标准的出台背景、实施意义、实施步骤、技术要点和法治理念等做深入解读。专家指出，《标识办法》《标识方法》明确相关服务主体的标识责任义务，规范内容制作、传播各环节标识行为，注重与现有治理机制衔接，构建了显式与隐式双层标识体系，以合理成本提高安全性，促进人工智能在文本对话、内容制作、辅助设计等各应用场景加快落地。未来，标识技术体系将不断完善，将强化内容风险分级及评估，构建健全内容标识制度建设和机制创新，防控人工智能生成合成技术滥用危害，防范利用人工智能技术制作传播虚假信息等风险行为，推动人工智能健康有序发展。当地企业代表在宣讲会上分享了推动标识法规标准落地的经验。在以“企业内容标识技术与合规”为主题的圆桌讨论环节，来自人工智能及相关领域的企业代表重点探讨了对“标识办法”的理解和认识，并提出对办法落地的思考与建议。

来自省市相关主管部门、科研院所、大模型企业、互联网平台等单位 100 多名代表参加宣讲会。与会代表表示，本次活动聚焦政策落地与实操应用，对人工智能生成合成内容合规管理和风险防范具有很强的指导价值，有利于支持企业人工智能健康发展，行稳致远。

网络产品安全能力提升计划获奖单位及个人名单发布

4 月 23 日，网络产品安全能力提升计划获奖单位及个人名单在第二届武汉网络安全创新论坛主论坛正式发布，中央网信办网络管理技术局主要负责同志、网络安全协调局主要负责同志以及武汉市相关负责同志为获奖单位及个人颁奖。

为深入贯彻落实习近平总书记关于网络强国的重要思想，特别是关于国产软硬件安全的重要指示精神，2024 年 8 月，中国网络空间安全协会联合电科金仓、中科方德、华为、金蝶天燕、金山、泛微、中创 7 家信创企业共同发起网络产品安全能力提升计划（以下简称“提升计划”）。提升计划先后确定 7 家信创企业的 10 款产品参与检测，协会先后组织“白帽子”对网络产品通过线上、线下检测确定有效漏洞，推动企业及时修复产品安全漏洞、更新升级产品，持续提升网络产品安全能力，在此活动中也涌现出一批优秀单位及个人（名单如下）。

网络产品安全能力提升计划获奖单位及个人名单

2024 年网络产品安全能力提升计划优秀人才单位

中国电子科技集团有限公司

中国联合网络通信集团有限公司

中国电信集团有限公司

中国移动通信集团有限公司

奇安信科技集团股份有限公司

北京天融信网络安全技术有限公司

杭州安恒信息技术股份有限公司

2024 年网络产品安全能力提升计划潜力人才单位

暨南大学

亚信安全科技股份有限公司

北京邮电大学

东南大学

深信服科技股份有限公司

2024 年网络产品安全能力提升计划优秀参与单位

山东中创软件商用中间件股份有限公司

深圳市金蝶天燕云计算股份有限公司

中电科金仓（北京）科技股份有限公司

泛微网络科技股份有限公司

华为技术有限公司

中科方德软件有限公司

珠海金山办公软件有限公司

2024 年网络产品安全能力提升计划突出贡献奖

特等奖

中国电子科技集团有限公司 陈司琪

一等奖

中关村实验室 张之义

北京天融信网络安全技术有限公司 闫伟进

中国移动通信集团有限公司 张泉

二等奖

北京天融信网络安全技术有限公司 陈青阳

中国联合网络通信集团有限公司 杨晓成、罗军

中国电信集团有限公司 孙少先

奇安信科技集团股份有限公司 陈瑞琦

杭州安恒信息技术股份有限公司 刘祥来

2024 年网络产品安全能力提升计划新锐奖

亚信安全科技股份有限公司 焦军勋

东南大学网络空间安全学院 孙典

暨南大学 陈耿灿

深信服科技股份有限公司 贾金岗

2024“黄鹤杯”网络安全人才创新大赛优秀成果专栏

01. 大赛介绍

为深入贯彻习近平总书记关于网络强国的重要思想，坚持网络安全教育、技术、产业融合发展，加快推动国家网络安全人才与创新基地高质量建设发展，形成人才培养、技术创新、产业发展的良性生态，推动网络安全产业高质量发展，助力超大城市网络安全防御体系打造。决定举办 2024 年“黄鹤杯”网络安全人才创新大赛。

02. 组织机构

指导单位：武汉市委网信办

主办单位：国家网络安全人才与创新基地

承办单位：武汉市网络安全协会

协办单位：网络和数据安全全国产才融合中心、黄鹤实验室、武汉攀升鼎承科技有限公司

03. 赛事介绍

（一）网络安全理论创新赛

面向个人及团队征集网络安全基础研究领域的理论创新成果。

（二）网络安全实践创新赛

面向网络安全企业征集行业典型应用场景下的解决方案或创新型产品。

04. 赛程安排

预赛（专家评审）时间：2024 年 12 月 12 日（周四）

决赛（线下路演）时间：2024 年 12 月 19 日（周四）

地点：国家网络安全人才与创新基地

05. 奖项设置

网络安全理论创新赛

- 一等奖 1 名
- 二等奖 2 名
- 三等奖 3 名
- 理论创新突破奖 1 名
- 理论前沿探索奖 1 名
- 理论价值学术奖 1 名

网络安全实践创新赛

- 一等奖 1 名
- 二等奖 2 名
- 三等奖 3 名
- 实践创新突破奖 1 名
- 实践行业推动奖 1 名
- 实践价值效益奖 1 名

附：2024 年“黄鹤杯”网络安全人才创新大赛获奖名单

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

智慧交通物联网数据协同异常检测方法：为未来交通安全保驾护航

孙思宇、邓云康、徐良松、朱苏文、秦书琪、王帅

华中科技大学网络空间安全学院　CPSS 战队

智慧交通是人工智能、物联网、大数据等新一代信息技术与交通运输深度融合的新业态。为实现“交通强国”和“智慧交通”发展目标，国家颁布了《交通强国建设纲要》、《国家综合立体交通网规划纲要》等一系列政策规范，智慧交通成为现代交通行业发展的新方向。然而，随着智慧交通物联网的规模化普及应用，其设备规模及生产数据呈指数级增长，传感器设备可产生大规模异构数据，这些数据中不可避免会出现由设备故障、系统错误或网络攻击（比如 DDOS 攻击、中间人攻击等）而导致的异常数据，导致了交通网设备计算效率下降、安全风险激增等问题，对智慧交通物联网的安全可靠运行构成严重威胁。因此，亟需根据智慧交通物联网数据特性及其应用场景，设计一种数据协同异常检测方法实现准确高效的数据异常精准检测，预防潜在危险，维护智慧交通物联网复杂应用环境下的数据安全。

项目背景与核心挑战

智慧交通物联网设备数据通常可以分为离散数据和时序数据，离散数据主要指智慧交通物联网中的通信流量，该通信流量中可能存在由多种多样的网络攻击产生的异常数据，而时序数据表示智慧交通物联网系统中多个传感器监测到的多变量时间序列，这些时序数据可以反映交通物联网设备情况，但传感设备故障、恶劣天气影响等不可控因素都有可能导致时序数据产生异常。针对两种不同类型的数据进行异常检测是确保智慧交通物联网平台性能情况稳定、安全、高效运行的关键环节。然而现有的数据异常检测算法仍然面临两大痛点问题：

1.1 离散数据异常：种类繁多且未知

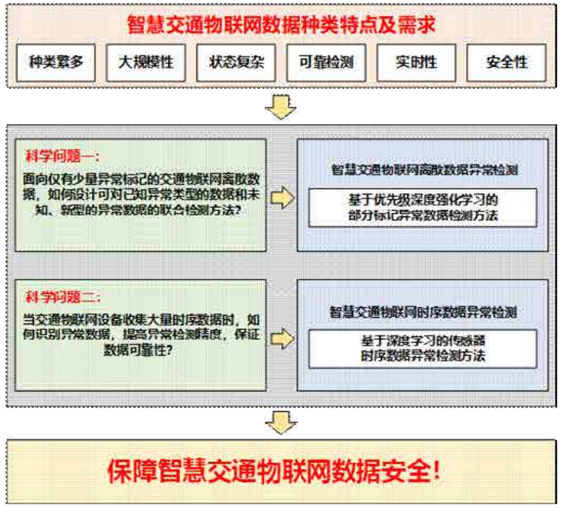
由于实际交通网环境的复杂性和数据采集的难度，很多离散异常数据往往没有明确的标签，或者仅存在极小量的标签。现有研究大多采用无监督学习的方法设计离散数据异常检测算法，但由于没有数据标签提供先验信息，无监督学习方法通常会造成误报或漏报异常数据的现象，导致异常检测的准确性较低。另外，现有基于半监督学习的异常检测算法泛化能力较弱，难以应对未知或新型的离散异常数据。因此，本作品考虑了当前智慧交通物联网应用中仍存在极小量异常数据标签的情况，设计可对已知异常类型的数据和未知、新型的异常数据进行联合检测的方法，提高离散异常数据检测的准确性和效率，为智慧交通物联网的安全运行提供有力保障。

1.2 时序数据异常：高维特征复杂关联

现有多变量时序数据异常检测的研究工作多数采用无监督学习方法提取正常数据特征，识别异常数据，未考虑智慧交通环境中传感器节点之间的相关性，也未考虑多变量时序数据的高维特征之间复杂的非线性关系导致的检测精度不足的问题。而深度学习方法可以自动对数据的潜在特征进行高效提取，建模传感器节点之间的关系，对异常数据进行高效识别。因此，本作品构建了基于深度学习的传感器多变量时序数据异常检测模型，突破复杂的非线性关系瓶颈，对节点收集的数据进行高维特征提取，学习传感器节点相关性，实现准确高效的异常数据准确检测，提升智慧交通物联网数据可靠性。

两大核心技术突破

针对上述挑战，华中科技大学 CPSS 战队提出了“智



慧交通物联网数据协同异常检测方法”，通过深度强化学习与深度学习的结合，实现了离散与时序数据异常的协同检测。

基于优先级深度强化学习的部分标记异常检测方法（PANDA）

技术原理：构建马尔可夫决策过程模型，将智能体与数据环境的交互转化为状态、动作、奖励的动态优化过程。利用深度确定性策略梯度（DDPG）算法和优先经验回放机制，结合少量已标记数据和大量无标记数据，实现已知异常的精准识别与未知异常的探索。

优势：

突破数据标注限制，仅需少量标签即可检测已知和新型异常。

通过优先级回放机制，智能体优先学习高价值经验，提升检测效率和鲁棒性。

在 UNSWNB-15、Shuttle 等数据集上，AUC-ROC 和 AUC-PR 指标较传统方法提升 3.0%-10.3% 和 10.0%-73.5%。

基于深度学习的传感器时序数据异常检测方法（VG-Net）

技术原理：结合变分自编码器（VAE）和图神经网络（GNN），构建“预测 - 重构”联合模型。VAE 捕捉数据的潜在分布，GNN 挖掘传感器节点间的时空关联，通过输入输出差异评估异常分数。

优势：

有效处理高维时序数据的复杂非线性关系，提升异常识别精度。

在 SWaT、WADI 等 8 个数据集上，F1 分数较现有方法提升 10%-20%，尤其在高噪声环境下表现优异。

应用成果：智慧隧道的“智能守护者”

CPSS 战队与湖北楚天高速数字科技有限公司合作，将上述技术应用于“数字孪生智慧隧道平台”，实现了对隧道内设备运行状态的实时监测与异常预警。

实际应用效果

精准检测：平台可同时检测离散数据（如网络攻击）和时序数据（如传感器故障）异常，准确率大幅提升。

快速响应：异常响应时间从传统方法的数小时缩短至分钟级，显著降低事故风险。

效率提升：隧道设备故障率下降 30%，综合养护成本降低 25%，为智慧交通运营提供了可靠保障。

企业评价

湖北楚天高速数字科技有限公司评价称：“CPSS 团队的技术突破为智慧隧道的安全运行提供了“智能大脑”，其创新性方法在复杂环境下展现了卓越的鲁棒性，为行业树立了新标杆。”

结语

在智慧交通的浪潮中，数据安全是基石，异常检测是关键。华中科技大学 CPSS 战队的创新方法，正以科技的力量守护着每一段旅程的安全与畅通。从隧道到城市，从现在到未来，他们的探索将为全球智慧交通的发展提供“中国方案”，引领行业迈向更加智能、安全的新纪元。

网络安全风险量化评估规范

周韬
武汉华康科技有限公司

引言

在数字经济高速发展的背景下，网络安全已成为保障企业数字化转型和社会稳定运行的核心要素。武汉华康科技有限公司凭借其自主研发的《网络安全风险量化评估规范》，在 2024 年“黄鹤杯”网络安全人才创新大赛中荣获理论创新赛二等奖。该成果针对当前网络安全风险“看不清、管不住”的行业痛点，提出了一套系统性、标准化的量化评估方法，为行业风险监管、企业安全管理和保险风控决策提供了科学依据。

一、项目背景与必要性

随着数字化进程加速，网络安全威胁日益复杂化，传统防护手段如防火墙、入侵检测等技术已难以应对动态风险。企业亟需从被动防御转向主动风险管理，通过量化评估提前预警潜在威胁。然而，当前市场缺乏统一的风险量化标准，导致评估结果难以横向比较，产品和服务存在技术壁垒。

在此背景下，武汉华康科技有限公司结合国家政策导向与市场需求，编制了《网络安全风险量化评估规范》。该规范响应了工信部《关于促进网络安全保险规范健康发展的意见》等政策要求，旨在解决三大核心痛点：

1. 数字生态风险监管难题：如何高效监管海量企业的数字基础设施安全？

2. 供应链安全管理挑战：如何管控成百上千第三方供应商的安全风险？

3. 保险风控决策需求：如何快速评估企业风险以支持网安险精准定价？

二、规范的核心内容与创新亮点

1. 系统性框架与标准化方法

规范采用“定量 + 定性”结合的方法，构建了涵盖风险识别、评估、控制和持续改进的全生命周期管理体系。通过建立多维指标体系（如风险等级、发生概率、影响程度等），实现了风险的精准量化与优先级排序，为企业资源分配和决策提供依据。

2. 技术创新与行业突破

新技术融合：整合人工智能、大数据和云计算技术，提升评估工具的自动化水平。例如，AI 算法用于威胁预测，大数据技术处理海量安全日志，云平台实现分布式计算与实时监测。

动态可扩展性：支持根据企业规模和业务场景定制评估模型，适配工业控制、交通、政务等不同领域需求。

风险共享机制：通过标准化指标促进跨组织信息共享，推动行业协同防御能力提升。

3. 政策合规与实践价值

规范严格遵循《网络安全法》《关键信息基础设施安全保护条例》等法规要求，并参考了多项国家标准（如

DB3212/T 1117—2022《政务数据安全风险评估规范》），确保评估流程的合规性与权威性。其实践价值体现在：

- 助力企业平衡安全投入与业务目标，降低不确定性；

- 为政府监管提供统一标尺，提升治理效率；

- 推动网安险产品创新，加速风险定价模型落地。

三、应用场景与实施路径

1. 典型应用场景

- 网络安全态势感知：通过量化评估实时识别外部暴露面漏洞，辅助安全人员快速定位威胁。

- 风险管理与应急响应：基于风险等级制定针对性控制措施（如技术加固、预案演练），缩短事件处置时间。

- 保险风控与合规报告：为保险公司提供可量化的风险评估报告，支撑承保决策；同时满足监管机构的安全合规报送要求。

2. 实施方法论

- 风险识别阶段：结合等级保护 2.0 体系，梳理关键信息基础设施和业务场景中的潜在风险点。

- 评估与量化阶段：采用贝叶斯推理、模糊综合评价等方法，计算风险值并生成可视化报告。

- 控制与改进阶段：建立动态监测机制，定期验证措施有效性，并通过态势评估报告持续优化策略。

四、行业影响与未来展望

该规范的推出填补了国内网络安全风险量化评估标准的空白，已在湖北省政务数据管理、工业控制系统等领域试点应用，显著提升了风险预警和处置效率。未来，华康科技将聚焦以下方向：

1. 技术深度融合：进一步探索 AI 驱动的实时风险评估模型，实现“监测 - 预测 - 响应”闭环。

2. 生态协同建设：联合高校、科研机构和高新企业，共建行业级风险共享平台。

3. 国际标准接轨：推动规范与国际标准（如 ISO/IEC 27005）对接，助力中国企业全球化布局。

结语

《网络安全风险量化评估规范》是华康科技在网络安全领域的重要创新成果，其科学性、实用性和前瞻性为行业树立了新标杆。未来，公司将持续深化技术研发与应用实践，助力构建更智能、更协同的数字安全生态，为数字经济高质量发展筑牢安全底座。


团 体 标 准

网络安全风险量化评估规范

Specification for Quantitative Assessment of Cybersecurity Risks

武汉市网络安全协会 发布

基于区块链的电力应用数据安全共享研究

覃思航　黄梦琦　李威

国网武汉供电公司信息通信分公司

2024 年 12 月 19 日，备受瞩目的 2024 年“黄鹤杯”网络安全人才创新大赛决赛在国家网安基地盛大举行。赛事紧密贴合时代发展脉搏，深度聚焦网络安全前沿趋势，精心设置了网络安全理论创新赛和实践创新赛两个赛道。国网武汉信通分公司根据专业特色和业务实际，申报了《基于区块链的电力应用数据安全共享研究》这一研究成果，与各大高校、企业队伍进行角逐竞争，最终荣获理论赛道二等奖。

一、研究背景

随着电力网络智能化发展，电力系统产生海量数据，这些数据分散存储于不同部门。数据共享面临诸多难题，如安全性差，存在数据篡改、用户越权、数据泄露风险；流转管控难，传统中心化存储和传输方式难以满足需求。在此背景下，区块链技术凭借其去中心化、分布式、难以篡改等特性，为电力应用数据安全共享提供了新途径。

二、研究现状

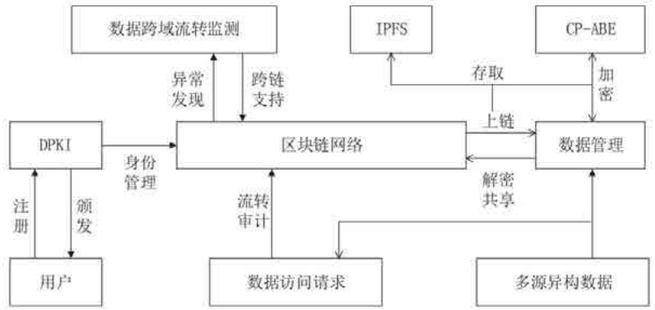
数据交换共享机制方面，传统依赖第三方服务商的模式存在数据泄露风险，数据持有者对第三方存防备心理。区块链技术虽被广泛应用于电力领域，如用于记录电力交易数据，但现有系统或缺乏可靠控制机制实现隐私交易数据安全访问，或未重视个人隐私，存在数据安全风险。

数据共享安全保证机制方面，当前研究在数据加密、身份认证、访问控制等方面存在不足。基于 IDB 加密的方案简化了证书管理流程，但存在恶意替换公钥风险；利用区块链提高证书透明度的方法，忽视了证书验证功能失效问题；现有访问控制机制难以灵活保证加密文件的可访问权限范围。跨链技术在电力数据跨部门交换共享中逐渐受到关注，但现有跨链技术多针对资产转移场景，不适用于数据共享场景下的用户隐私数据跨链共识与监测、溯源。

三、基于区块链的电力应用数据安全共享系统设计

（一）系统整体架构

从数据交易流程和平台运行全生命安全周期角度出发，PDTS 系统基于联盟链框架与电力机构数据平台搭建。系统采用区块链结合属性密码的方法，利用 ABE 加密技术，将用户属性作为权限构成基本元素，同步属性授权与加解密过程。通过分布式数字身份 DID 管理用户身份，密文存储在星际文件系统 IPFS 中，链上仅存储密文哈希，同时在 mongodb 数据库备份。用户



PDTS 系统

经区块链背书获取文件地址并申请解密。

（二）数据访问控制机制与安全保障

身份认证机制：用户身份注册采用投票制，由联盟链管理者投票决定。身份注册信息包括账号名、密码等多种元数据，用户证书采用 X.509 标准证书，以 BASE64 编码格式保存于区块链，通过证书解析函数获取有效期。智能合约检验证书，过期或撤销的证书对应用户行为受限。

数据确权与权限共享：属性密码是数据共享关键，其管理涵盖创建、申请、授权及撤销流程。属性授权中心初始化全局属性，确保属性唯一标识。用户申请属性时，系统生成标识上链，授权中心处理后将属性添加到申请者集合，更新哈希并加密生成新证书。

数据受控流转：传统 CP-ABE 算法在电力系统应用存在性能瓶颈，本系统在其基础上增加区块链数据流转审计。用户访问文件时，智能合约先验证用户权限，匹配成功后返回文件存储地址，用户获取密文验证哈希后解密，避免用户随意尝试解密浪费资源。

（三）数据的隔离与审计监管机制

系统通过中心链进行安全策略分发、跨域数据交换管控与审计监管。跨域数据交换经细粒度权限管理系统管控后记账并在中心链达成共识，支持行为追溯。数据交换溯源可查询文件操作信息。系统设置监管者角色，通过智能合约审计发现异常，标记上链并告警。同时，设计数据追溯功能，构建属性共享、数据流转和用户行为路径，方便监管人员查看。

四、实验设计与结果分析

实验在国网武汉供电公司电力应用系统进行，基于 Hyperledger Fabric V1.4 搭建区块链网络，使用多种框架和语言开发系统各部分。

功能测试表明，用户注册、属性授权等关键步骤耗时满足实际需求，策略复杂程度对数据上传性能影响较小，系统更适用于小文件共享交换，跨链数据共享事务时耗小于 250ms，能拦截不满足权限的请求。

性能测试显示，属性密码创建、加密策略标识上链、用户解密请求标识上链等事务处理性能稳定在 350TPS 以上，事务查询 TPS 可达 1000 以上，跨链事务处理性能相对单链事务较差，但可并发执行，中心链承担业务链过多时性能下降，文件上传大小增长对区块链并发性能影响不大。

五、研究总结

基于区块链的电力应用数据安全共享系统，有效解决了电力数据共享中的安全和流转管控问题。通过创新的访问控制机制、跨链机制和文件流转方法，提高了系统安全性和效率。未来可进一步划分数据安全等级，结合零知识证明技术加强隐私安全，以更好地满足电力网络数据共享的需求。

基于群决策的共识自适应信任管理

张泽林、王浩翔、宋宇杰、曹越、
武汉大学国家网络安全学院　ASAP 课题组

1 研究背景与现状

随着泛在智联技术的快速发展，车联网作为智能交通的核心应用场景，面临开放性和复杂性带来的多元信任威胁，如虚假消息注入、信任操控等，可能导致数据篡改、网络实体不互信，甚至引发交通失调、车辆失控等严重后果。在此背景下，信任管理成为保障网络安全和数据可靠传输的关键技术，受到广泛关注。

目前，信任管理研究主要集中在基于贝叶斯理论、DS 证据理论的可信度评估与信任建模。这些方法为网络实体行为和信任关系提供量化手段，但存在诸多局限性。首先，现有方法多依赖静态或半动态模型，难以适应网络环境的快速变化；其次，DS 证据理论在处理不确定性信息时，信任模型的动态调整和阈值管理能力不足。此外，现有研究多聚焦于路侧单元协助的可信度评估，缺乏对高动态性自组网的信任评估解决方案。

因此，为突破传统信任评估维度不足、信任阈值固化、高危环境失效等领域壁垒，本成果提出了一项基于群决策的共识自适应信任管理方案，探索决策理论与信任管理技术的深度融合，为车联网安全提供高效、动态、可靠的信任管理机制，推动智能交通领域的发展。

2 理论成果介绍

2.1 多方位的共识水平评估

为突破传统信任评估维度不足，本研究通过引入多方位的共识水平评估，从不同角度量化信任差异，从而更全面地反映信任状态。通过构建主观共识水平、客观共识水平、综合共识水平和自证共识水平四个维度，全面量化车辆之间的信任差异。其中，主观共识水平基于评估者自身的意见，客观共识水平基于评估者邻居的意见，综合共识水平则结合了主观和客观维度，而自证共识水平由被评估车辆自身提供，用于验证其可信性。这种多维度评估方式突破了传统单一维度信任评估的局限性，能够从不同角度反映车辆的信任状态，有效提升信任评估的准确性和可靠性，为车联网中的信任管理提供了更全面的视角。

2.2 动态阈值机制

动态信任阈值调整机制用于解决信任阈值固化问题。该机制根据车辆的反馈信息、信任容忍度以及群体意见的权重，动态调整信任阈值，从而更好地适应车联网中不同规模和动态变化的网络环境。信任阈值能够根据车辆的交互历史、群体意见的可信度以及评估者的主观信任偏好进行灵活变化。例如，当评估者对自身意见更有信心时，会更依赖自身的信任容忍度；而当评估者对邻居意见较为信任时，会更多地参考邻居的信任容忍度。通过这种动态调整方式，信任阈值能够根据车辆的交互历史、群体意见的可信度以及评估者的主观信任偏好进行灵活变化。这不仅提高了信任评估的适应性和准确性，还增强了系统在面对不同网络环境和恶意行为时的鲁棒性。

2.3 信任担保机制

本研究通过引入担保信任来增强车联网中信任评估的可靠性和效率。在这种机制下，评估车辆可以为其邻居车辆提供信任担保，担保车辆通过自身的信任评估为被担保车辆的可信性提供额外的保证。这种担保行为不仅扩大了信任评估的范围，还能够快速识别潜在的恶意车辆。当评估车辆对被评估车辆的信任度存在不确定性时，担保车辆的积极意见可以作为参考，帮助评估车辆做出更准确的判断。同时，担保机制通过惩罚和奖励机制来激励车辆提供真实可靠的意见，从

而提高整个车联网的信任管理系统的鲁棒性和安全性。这种机制特别适用于车联网这种高动态、高风险的环境，能够有效减少恶意行为对信任评估的影响，确保车辆间的安全通信。

2.4 群决策机制

最后，群决策机制用于优化车联网信任管理，通过模拟群体决策过程，动态调整车辆的信任值以达成共识。车辆作为决策者，基于自身和其他车辆提供的意见（信任评估信息），通过多轮迭代调整自己的信任观点，以减少意见分歧并最终达成一致。这一过程不仅考虑了个体车辆的意见，还通过聚合群体的智慧，增强了信任评估的准确性和可靠性。此外，群决策机制通过引入意见调整和共识达成过程，能够有效应对车联网中车辆的高动态性和复杂交互环境，同时为信任管理提供了更灵活、更具适应性的解决方案，显著提升了系统在面对恶意行为和动态变化时的鲁棒性。

2.5 科学性验证

研究通过大量仿真实验，从多个关键指标（包括准确性、精确率、召回率和 F1 分数）对方案进行了全面评估。实验结果表明，该方案在高风险场景下表现出色，能够有效识别恶意车辆并保障数据传输的安全性。与现有的方法相比，在准确性、精确率、召回率和 F1 分数等方面均显著优于其他方法，证明了其在动态车联网环境中的优越性。

3 研究团队

武汉大学国家网络安全学院 ASAP 课题组由曹越教授领衔（国家级青年人才、国家重点研发计划青年首席科学家、英国皇家特许工程师、英国计算机学会会士、英国高等教育学会会士、英国皇家学会工艺院会士、英国计算机学会会士），团队成员包含 12 名博士、14 名硕士，面向智能交通领域主要开展网络安全、网络通信、决策优化等技术研究，涵盖车联网及低空经济等应用场景。团队成员相关研究成果发表于国内外知名期刊。本项目成果完成人包括：张泽林，王浩翔，宋宇杰，曹越。

群智感知的数据安全

张明武　张媛媛　王玉珠　沈华
湖北工业大学网络空间安全研究所

2024 年年末，在“黄鹤杯”网络安全人才创新大赛上，由张明武教授带领的湖北工业大学网络空间安全团队凭借作品《群智感知的数据安全保护机制研究》脱颖而出，荣获三等奖。团队成员张明武、张媛媛、王玉珠和沈华，针对当前备受关注的群智感知应用场景，提出了两个极具创新性的保护数据安全的方案，为数据安全保护领域注入了新的活力。

群智感知：物联网感知的新范式

那么，什么是群智感知呢？这是一种将移动感知和众包思想相结合的新型物联网感知范式。它以大量普通用户使用的移动设备作为基本感知单元，通过物联网和移动互联网的协作，实现感知任务的分发与数据的收集利用，最终完成大规模、复杂的社会与城市感知任务。群智感知的应用场景极为广泛，涵盖了环境监测、智能交通、智慧医疗和智慧城市等多个领域，为智慧社会的建设提供了强大的技术支持。然而，群智感知在带来便利的同时，也面临着数据安全的挑战。如何在利用群智感知技术的同时，确保数据的安全性和隐私性，成为了湖北工业大学团队的研究重点。

创新成果：守护数据安全的利器

隐私增强型联邦学习聚合方案

湖北工业大学团队的第一个代表性成果是群智感知系统中的隐私增强型联邦学习聚合方案。该方案巧妙地结合了哈希 Diffie-Hellman 交换协议和同态加密技术，并引入了基于数据打包技术的编码与聚合方法。这一创新不仅有效降低了计算和通信成本，还大大增强了数据的隐私保护能力。相关成果发表在了 CCF A 类、中科院 1 区的期刊《IEEE Transactions on Information Forensics and Security》上，得到了学术界的广泛关注和认可。

安全电子医疗决策树评估方案

湖北工业大学团队的第二个代表性成果是一种创新的安全电子医疗决策树评估方案。在医疗领域，精准的疾病分类诊断至关重要，但同时也涉及到患者的敏感生理信息和医疗服务商的决策树算法模型的保护问题。湖北工业大学团队提出的这一方案，在实现精准疾病分类诊断的同时，确保了参与者的敏感生理信息及医疗服务商的决策树算法模型得到严格保护。该成果发表在了 CCF A 类、中科院 2 区期刊《IEEE Transactions on Dependable and Secure Computing》上，为电子医疗保健系统中的隐私保护提供了新的思路和方法。

创新与科学：筑牢数据安全防线

在理论上，团队针对移动群智感知场景提出了一种隐私增强联邦学习方案，为电子医疗保健系统中的隐私保护决策树评估提供了一种全新的方案。这些理论成果为后续的研究提供了重要的参考和借鉴，推动了相关领域的理论发展。在技术层面，抗合谋设计和数据编码方法为隐私增强技术奠定了坚实的基础。这些技术的创新推动了隐私保护技术和决策树分类算法

在医疗领域的交叉融合，促进了相关学科的发展，为解决复杂的数据安全问题提供了新的技术手段。湖北工业大学团队的研究成果对智慧城市、健康监测等依赖群智感知的实际应用具有重要的指导意义。这些方案不仅能够有效保护数据安全，还能提高系统的运行效率，为智慧社会的建设提供了有力的技术支持。此外，相关成果多次被知名专家学者团队引用，包括但不限于冯登国院士团队及入选“新世纪百千万人才工程国家级人才”的廖晓峰教授团队，充分证明了其在学术界和实际应用中的重要影响力。

团队风采：荣誉与成就

湖北工业大学网络空间安全团队是一支在数据安全领域具有深厚积累和丰富经验的团队。近年来，他们先后获得了省科技进步二等奖（2003 年）、自然科学三等奖（2014 年）、科技进步三等奖（2015 年）、武汉市科技进步二等奖（2015 年）等多项荣誉，充分展示了他们在科研领域的卓越实力。在学术研究方面，团队取得了丰硕的成果。他们共发表论文 200 余篇，出版学术专著三部、译著四部，申请专利 80 余件，其中授权国际和国内专利 40 余件，软件著作权登记 20 余件。这些成果不仅为团队赢得了声誉，更为数据安全领域的发展提供了重要的理论和技术支持。值得一提的是，团队还实现了专利转化 7 项。这些专利转化不仅为团队的科研工作提供了资金支持，更为相关技术的推广应用提供了有力保障。基于本次获奖的两篇论文，团队也申请并授权了相关专利，进一步巩固了他们在数据安全领域的领先地位。

结语

湖北工业大学网络空间安全研究所的团队在“黄鹤杯”网络安全人才创新大赛中取得的优异成绩，不仅是对他们研究成果的肯定，更是对他们多年来在数据安全领域不懈努力的回报。他们的研究成果不仅在理论上具有创新性，在技术上具有科学性，更在应用上具有极高的价值，为群智感知场景下的数据安全保护提供了全新的思路和方法。我们期待他们在未来能够继续发挥专业优势，为数据安全领域的发展贡献更多的智慧和力量，守护好我们数字世界的每一道防线。

基于改进 YOLOv9 的智能网联汽车图像脱敏系统

杨子旭 [1] 王依婷 [1] 赵诗语 [1] 秦灏阳 [1] 裴昊天 [1] 胡林 [2]

[1]（湖北大学网络空间安全学院）

[2]（湖北大学计算机学院）

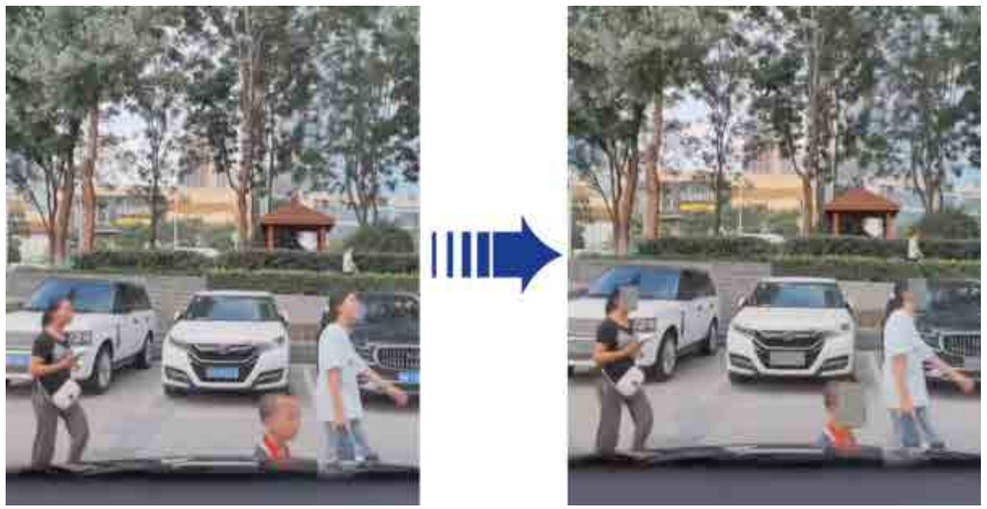
1. 背景意义

智能网联汽车作为前沿科技与传统汽车产业深度融合的产物，是我国汽车产业转型升级的重要战略支撑。然而，其广泛应用带来了数据安全与隐私保护的严峻挑战。近年来，特斯拉哨兵模式等智能网联汽车的数据泄露事件频发，引发了对隐私安全的广泛关注。我国陆续出台了《关于加强车联网网络安全和数据安全工作的通知》《汽车数据安全管理若干规定》及《网络安全标准实践指南》等法律法规，要求对汽车数据传输过程中的敏感信息进行脱敏处理，以确保数据安全与合规。

在此背景下，智能网联汽车图像脱敏问题本质上是复杂交通环境下的多目标检测与识别问题。既要做到准确识别车牌和人脸等敏感信息，又要在恶劣环境下保证检测的稳定性和实时性。本系统依托于湖北大学网络空间安全学院以及湖北大学智能感知系统与安全教育部重点实验室等多个科研平台的支持，获得了丰富的科研资源与学术指导，为项目的顺利开展与技术优化提供了重要保障。

2. 核心技术

本系统基于 YOLOv9 模型，并在其原有的 PGI 与



GELAN 模块基础上进行优化，以提高其在复杂场景下的检测精度与稳定性。YOLOv9 模型中的 PGI 模块通过辅助可逆分支和多级辅助信息增强特征学习效果，GELAN 模块则通过添加可逆分支，增强对目标的关注能力。然而，在实际应用中，YOLOv9 在遮挡、形变、光照变化等复杂场景中的检测效果仍有待提升。为此，本系统提出了以下改进措施：

结合自适应 NMS 算法对检测过程进行优化，通过根据候选框数量自适应调整高斯衰减函数的应用，以对重叠检测框的置信度进行连续性衰减而非简单删除，从而提升目标遮挡情况下的检测精度与召回率。相比于传统 NMS 方法，自适应 NMS 算法在智能网联汽车的复杂场景中表现出更高的鲁棒性与准确性，为动态环境下的目标检测提供了更可靠的技术支持。

其次，为应对形变目标的检测，本系统优化了 YOLOv9 模型中卷积模块的操作，采用可变核卷积替代传统卷积。可变核卷积能够自适应调整卷积核的大小与形状，从而精准捕捉不同形变的目标特征，尤其在车辆转弯、变道等复杂场景中表现出色。

此外，为了提升系统在复杂光照环境中的检测效果，本系统引入了 FFT-MSRCR 图像增强算法。通过将快速傅里叶变换与多尺度 Retinex 算法相结合，并引入色彩恢复因子 C，显著提高了光照不足、过强或视野模糊等环境下的图像质量，为后续的目标检测提供了更优的输入。

在敏感信息脱敏处理方面，本系统采用了基于 XOR 的像素级一次一密加密算法对检测到的车牌和人脸区域的 R、G、B 三通道数值进行处理，实现对图像数据的高效脱敏。同时，使用自定义 LSB 的信息嵌入算法嵌入相关参数，以便在必要时于公安机关的监管下实现数据恢复。

3. 实际应用

项目组成员为了进一步提升系统的检测精度与鲁棒性，精心采集了超过 6 万张涵盖多种复杂交通场景的图像数据。这些场景不仅包括常规环境，还涉及强弱光条件、目标遮挡与形变、视野模糊等多种极端情况。经过细致的人工标注与处理，项目组构建了一个高质量且多样性丰富的数据集，为 YOLOv9 模型的训练与优化提供了强有力的支持。得益于这一自建数据集的高质量与广泛覆盖，模型的泛化能力与检测效果得到了显著提升。

本系统的应用潜力远不止于智能驾驶。在安防监控、低空经济、智慧交通等多个领域中，它都展现出卓越的适应性与实用性。无论是对智能驾驶中图像数据的实时脱敏处理，安防监控中对敏感信息的精准保护，还是低空经济与智慧交通中对关键数据的高效加密与传输，本系统都能够提供稳定而高效的解决方案。

值得一提的是，本系统自建的数据集已引起襄阳达安汽车检测中心有限公司的关注，并表达了对其在智能网联汽车图像脱敏技术测试中应用的潜在需求。通过与行业领先企业的合作意向对接，我们正积极探讨数据集在真实场景下的验证与优化可能性，以期进一步提升系统的实用性与准确性，为未来的产业化应用奠定坚实基础。

4. 结束语

基于改进 YOLOv9 的智能网联汽车图像脱敏系统通过引入自适应 NMS 算法、可变核卷积、FFT-MSRCR 图像增强技术以及基于 XOR 的像素级加密算法，实现了对复杂场景下车牌和人脸等敏感信息的精准检测与脱敏。系统不仅在公开数据集上取得了优异的性能表现，还能在自建数据集的复杂场景中保持稳定的检测效果。

未来，本系统将在智能驾驶、无人机应用、智慧交通等领域进一步推广与优化，为保障数据安全与隐私保护提供更加完善的技术解决方案。

《湖北省重要网络和信息系统密码应用技术指南》的理论创新成果

李荣及该标准编制组

引言

密码是保障网络安全的核心技术和基础支撑，在网络安全防护中具有不可替代的作用。在国际国内网络空间安全形势日益严峻的环境下，重要网络和信息系统如何合规、正确、有效地应用密码技术保障系统安全，成为亟待解决的问题。为贯彻落实《中华人民共和国密码法》、《商用密码管理条例》等法律法规及政策文件的相关要求，同时也为了解决部分重要网络和信息系统运营者对于如何运用密码技术缺乏较为深入理解的问题，《湖北省重要网络和信息系统密码应用技术指南》编制组在 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的标准基础上，结合重要网络和信息系统的通用性密码应用需求，编写了该指南。

一、指南理论成果介绍

《湖北省重要网络和信息系统密码应用技术指南》提出了重要信息系统密码应用技术指南，包括密码应用实施总体框架、密码应用技术指南概述和具体实施方式，适用于重要信息系统规划、建设、运行各个阶段，为重要信息系统的规划设计、建设实施和运行维护过程中合规、正确、有效地应用密码技术，保障重要信息系统安全提供指导。《湖北省重要网络和信息系统密码应用技术指南》包括密码应用实施总体框架和密码应用技术指南两个部分。密码应用实施总体框架部分对于密码应用实施的通用技术框架、“三同步”的生命周期以及商用密码应用安全性评估等方面进行了描述；密码应用技术指南部分则从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全四个层面对于密码应用技术基本要求指标进行了解读，并给出了多个不同的具体实施指南，从部分方案到工作流程以及密码管理实现都做了详细的说明。

二、指南的创新亮点

《湖北省重要网络和信息系统密码应用技术指南》除了对密码应用实施总体框架和密码应用技术基本要求进行解读之外，更重要的是针对不同的安全层面提供了可参考的具体实施案例。每个实施案例首先描述其部署方案并附有部署示意图帮助重要信息系统责任单位理解密码设备部署位置和接入方式，然后详细描述密码应用工作流程同时也附有工作流程图帮助重要信息系统责任单位理解其技术原理，最后从密钥全生命周期的角度给出了密钥管理实现的参考，大大增加了了指南的可参考性和落地性。

三、指南的科学性

《湖北省重要网络和信息系统密码应用技术指南》严格遵循《中华人民共和国密码法》等相关法律法规，确保密码应用的合法性和规范性，参考并引用了信息安全技术和密码技术相关多个国家标准和行业标准，确保技术要求和实施方式与现有国家、行业标准体系相一致。《湖北省重要网络和信息系统密码应用技术指南》提供了一个结构化的密码应用实施框架，从总体要求到具体实施细节，逻辑清晰，层次分明。综合考虑了信息系统的各个方面，包括物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等。根据信息系统的安全等级，提供了分等级的密码应用技

术要求，确保了指南的适用性。不仅提出了密码应用技术基本要求的解读，还针对每个安全层面给出多个具体实施方式参考案例。案例包含密码应用部署方案、密码应用工作流程和密钥管理实现等内容，确保了指南的科学性、合理性和可操作性。

四、行业影响与未来展望

《湖北省重要网络和信息系统密码应用技术指南》作为湖北省商用密码协会发布的团体标准，它为湖北省重要网络和信息系统的规划设计、建设实施和运行维护过程中合规、正确、有效地应用密码技术，保障重要信息系统安全提供了指导，同时也湖北省商用密码从业人员在密码应用安全领域的研究和实践提供了指导。该标准的制定和实施将促进省内外学术交流，为外省密码应用相关团体标准的制定提供了参考。同时该标准将理论研究与实际应用相结合，提供了一个将理论成果转化为实际应用的范例，推动湖北省密码行业产学研用深度融合，在未来在学术和实践领域都将发挥重要作用。

结语

《湖北省重要网络和信息系统密码应用技术指南》是商用密码领域的重要创新成果，它不仅为重要网络和信息系统运营者在使用密码技术过程中提供了全面、系统的指导，还为密码技术的学术研究和实践应用提供了有力支持。随着该标准的不断推广和应用，它将在保障重要信息系统安全、推动密码技术创新和发展等方面发挥更加重要的作用。

制造业数据安全管理中的数据分类分级方法指南团标深度解读

梁忠辉

智网安云（武汉）信息技术有限公司

在数字化浪潮中，制造业加速迈进转型之路，数据已然成为企业核心资产，其安全与否直接关系到企业生存与发展。在此背景下，武汉市网络安全协会重磅推出《制造业数据安全管理中的数据分类分级方法指南》团体标准（以下简称“团标”），由智网安云（武汉）信息技术有限公司牵头编制，为制造业数据安全管理打造了一套极具价值的规范，本团标旨在为制造业企业提供一套科学、合理、可操作的数据分类分级方法，助力企业提升数据安全管理水平。

本团标聚焦制造业，充分考虑了制造业企业的数据特点和业务需求。制造业数据具有多样性、复杂性和实时性等特点，涉及研发设计、生产制造、经营管理、运维服务等多个环节。团标针对这些特点，对制造业数据进行了详细分类，包括研发数据域、生产数据域、运维数据域、管理数据域和外部数据域等，为企业准确识别和管理各类数据提供了清晰的指引。

本团标采用了科学的数据分级方法，根据数据遭篡改、破坏、泄露或非法利用后，可能对企业生产、经济效益、社会稳定乃至国家安全造成的潜在影响程度，将数据分为核心、重要、一般。通过量化潜在影响因素，为企业提供了客观、准确的数据分级依据，有助于企业合理分配数据安全防护资源，实现数据的差异化保护。

本团标在制定过程中，充分结合了企业实际应用场景，注重标准的可操作性和实用性。标准不仅明确了数据分类分级的原则、方法和流程，还提供了详细的案例和模板，方便企业参考和实施。同时，团标还考虑到企业数据的动态变化，要求企业定期对数据分类分级结果进行复查和更新，确保标准能够适应企业业务发展和数据安全环境的变化。

一、本团标具有显著创新性：

（一）融合前沿技术与行业特性

本团标创新性地将新兴技术理念融入制造业场景。例如，借助大数据分析技术，对海量制造业数据进行智能分类。通过对数据生成频率、关联业务流程等多维度分析，实现精准分类，大幅提升数据处理效率，区别于传统依靠人工经验的分类模式。在数据分级方面，引入人工智能算法，基于数据被攻击后的模拟风险评估，动态调整数据级别。当企业引入新的智能制造生产线，相关生产数据风险评估更为智能、及时，确保数据安全防护始终贴合企业实际情况。

（二）构建动态管理机制

传统数据分类分级标准多为静态，难以适应制造业快速变化的业务。本团标打破这一局限，构建动态管理机制。随着企业业务拓展、技术升级，数据重要性和风险程度不断改变。团标要求企业定期重新评估数据，如企业开拓新市场，涉及的客户数据、市场调研数据等需重新分类分级，保障标准持续适配企业发展。同时，与行业动态安全威胁情报对接，当出现新型针对制造业数据的攻击手段，可及时调整数据安全防护策略，确保数据安全管理与时俱进。

二、本团标推广价值明显

（一）提升企业数据安全管理水平

通过实施本团标，企业能够对自身数据资产进行

全面梳理和分类分级，明确不同数据的安全保护需求，从而制定针对性的数据安全策略和防护措施。这有助于企业提高数据安全防护的精准性和有效性，降低数据安全风险，提升整体数据安全管理水平。

（二）促进数据合规使用与共享

在数据合规性日益重要的背景下，本团标为企业提供了符合法律法规要求的数据分类分级方法，帮助企业更好地满足数据安全监管要求，实现数据的合规使用。同时，合理的数据分类分级也为企业数据共享提供了基础，企业可以根据数据级别和共享需求，制定相应的共享策略，在保障数据安全的前提下，促进数据的流通和价值挖掘。

（三）推动制造业数字化转型

数据是制造业数字化转型的关键驱动力。团标通过规范数据管理，为企业数字化转型提供了坚实的数据安全保障。企业能够更加放心地利用数据进行创新应用，如工业互联网、智能制造等，推动业务流程优化和产品服务升级，提升企业核心竞争力，促进制造业数字化转型的深入发展。

三、本团标发布意义重大

（一）填补行业空白

目前，国内针对制造业数据分类分级的标准尚不完善，本团标的发布填补了这一领域的空白，为制造业企业开展数据分类分级工作提供了重要的参考依据，有助于规范行业数据安全管理行为，提升整个制造业的数据安全防护水平。

（二）引领行业发展

作为团体标准，本团标具有创新性和前瞻性，能够引领制造业数据安全管理的发展方向。通过在行业内推广应用团标，将促使企业不断优化数据管理流程，加强数据安全技术创新和应用，推动制造业数据安全管理向规范化、标准化、智能化方向发展。

（三）保障产业安全

制造业是国家经济的重要支柱，数据安全关乎制造业的稳定发展和产业安全。团标的实施有助于提升制造业企业的数据安全防护能力，防范数据泄露、篡改等安全事件的发生，保障制造业产业链供应链的安全稳定，为国家经济安全提供有力支撑。


ICS 35.240.01
L6440

团　　体　　标　　准

T/WHCSA 003—2024

制造业数据安全管理中的数据分类分级方法指南

Guide to data classification and grading methods in data security management of manufacturing industry

2024-11-26 发布　　2025-1-1 实施

武汉市网络安全协会　发布

云上数据泄露风险侦察技术

陈佛忠

神州绿盟武汉科技有限公司

作者介绍：陈佛忠，中共党员，绿盟科技高级安全研究员、中国通信学会高级会员。多次在知名会议上发表主题演讲，发表多篇论文、专利及白皮书，出版著作《数据要素安全：新技术、新安全激活新质生产力》。

1. 技术概述

近些年，很多企业为了降低业务运营成本、提升业务运营效率，纷纷上云。然后有些企业员工安全意识薄弱，在云化的过程中并没有注意安全问题，容易给企业带来意想不到的数据泄露的风险。除此之外，云上的组件和服务的网络属性具有个性化的特点，难以通过常规手段或在公共平台发现此类组件和服务。因此，数据泄露事件的“高发区”也在逐渐向云上迁移。此类云上数据泄露事件具备一定的隐蔽性，传统数据泄露情报监测手段（如暗网、论坛、Telegram 等）较难发现此类数据泄露事件。

针对上述现状，我们提出了一种云上数据泄露风险侦察技术，能够持续发现、识别某一区域内云上自建组件及公有云服务可能存在的数据泄露风险，该技术能力作为对传统数据泄露情报源的补充，可以很好地帮助监管机构对辖区内存在的此类数据泄露风险进行治理，更及时地避免数据泄露事件给公民、国家造成安全影响。

2. 创新性及核心能力

常规的数据泄露情报来源通常为暗网、论坛等渠道，此类情报属于“事后情报”。涉事企业和监管机构往往处于被动，难以定位到泄露主体和泄露途径，更加难以治理。云上数据泄露风险侦察技术发现的风险属于“事前情报”，拥有清晰的泄露路径和泄露主体，容易对其进行治理。 该技术首次系统性地对云上组件、服务的数据泄露风险进行研究。技术研究覆盖范围广，涵盖从自建服务到公有云服务等多个领域，包括 DevOps 服务、存储类服务、消息中间件、对象存储服务和云盘等。同时，纵向研究上聚焦造成组件、服务发生数据泄露风险的核心，提出了多种云上组件、服务的数据泄露风险分析、利用方法。

具体来说，云上数据泄露风险侦察技术拥有 5 个核心能力：

1. 基于资产聚类的云上组件识别发现能力：通过自研扫描引擎结合开源情报，全面获取互联网资产暴露情况，并依托自研指纹聚类技术，实现精准的组件、服务类型识别。同时，通过历史资产数据比对与动态资产变化分析，提升资产发现的完整性和时效性，支持多云环境下的资产统一识别与归类。

2. 基于动、静态扫描的云上组件风险发现能力：采用静态特征匹配和动态行为验证相结合的方式，对云上组件的配置缺陷、已知漏洞、未授权访问、弱口令风险以及潜在的数据泄露风险进行全面分析和利用验证，增强组件安全风险的自动化识别能力，支持一键验证风险的可利用性及影响范围评估。

3. 基于 AI 的敏感信息挖掘能力：结合机器学习、自然语言处理和规则匹配技术，对泄露数据进行深度

解析，自动挖掘其中可能包含的敏感信息，如用户身份信息、业务机密、密钥令牌、API 凭据等。同时，通过强化学习优化模型，提高不同语境和格式下敏感信息的识别精度，降低误报率，确保数据泄露风险的精准评估。

4. 基于多源融合的云上泄露数据社会域映射能力：融合域名解析、网络资产关系、组织注册信息等多源情报，对暴露的云上组件和服务进行社会域映射，精准定位其所属的组织机构和责任主体。同时，结合业务流量分析，进一步解析组件的业务属性，识别其可能涉及的行业或业务系统，提升对泄露数据影响范围的研判能力。

5. 基于 LLM 的泄露事件报告生成能力：利用 LLM 结合知识图谱和安全情报分析能力，自动归纳泄露事件的影响范围、涉及资产、潜在攻击手法及可行的安全防护建议，形成结构化、可读性强的安全报告。同时，基于推荐算法和实时情报订阅机制，一旦发现新的情报或泄露事件，能够自动生成并推送定制化报告给相关责任人，确保快速响应和处置。

3. 小结及展望

云上数据泄露风险侦察技术构建了一套完善的数据泄露风险分析体系，结合资产聚类、动静态扫描、AI 敏感信息挖掘、多源融合社会域映射等关键技术，实现云上组件和服务的精准识别及风险发现。该技术能够有效弥补传统数据泄露情报源的不足，帮助监管机构更全面地监测和治理云上数据泄露风险，避免数据泄露对国家及公民安全造成影响。

随着企业云化进程加快，安全意识不足及云上组件的特殊网络属性使得数据泄露风险进一步加剧，并逐步向云端迁移。由于其隐蔽性，传统情报监测手段难以有效识别。该技术依托 LLM 自动生成泄露事件报告，并结合实时推送机制，确保数据泄露情报的高效传递和快速响应，为云上数据安全提供有力支撑。

电子政务外网安全防护解决方案

中国电信股份有限公司武汉分公司

政务行业数字化转型下的安全挑战

中国数字政府建设已进入数据要素引领的智能时代（数字政府 2.0 阶段），随着国家“互联网 + 政务服务”的大力推进，政务外网作为电子政务重要基础设施，承载着全国政务非涉密信息系统的网络化运行，满足各级政务部门社会管理、公共服务等面向社会服务的需要。随着国家推进政务外网的整合，各级电子政务外网承载的业务系统越来越多，资产越来越庞杂，管理越来越复杂，并且由于电子政务系统业务价值高，面临的攻击形势也日益严峻，传统安全手段面临严峻挑战。

云网融合筑牢数字底座，助力政务外网安全

2023 年 6 月，武汉市正式发布了《武汉市数字政府和智慧城市建设三年行动方案 (2023-2025 年)》。《方案》规划了加快建设基础支撑、数据资源、城市治理、利企便民、政务运行等 5 大体系，明确了升级“云、网、数、智、端”智慧城市底座等 24 项工作任务。

电子政务外网安全防护解决方案，由中国电信武汉分公司精心打造的“云边端服一体化防护”的解决方案。基于中国电信的网络优势和运营经验，构建云侧运营分析、边侧威胁阻断、端侧贴身防护的“云边端服”联动的网络安全立体防护体系，实现了网络安全态势的实时监控与智能响应。

东湖高新区电子政务外网优秀创新实践

东湖高新技术开发区为武汉市经济增长提供了重要支撑，也是科技创新的核心区域。东湖高新区政务中心也积极进行数字政府建设，依托物联网、大数据、人工智能等前沿技术，提升了政务服务水平，推动了城市治理与经济发展的双赢。

为了加强区电子政务外网的安全防护能力，中国电信武汉分公司与东湖高新区政务中心进行了深度合作，最终在区电子政务外网中实践落地。

基于 MSSP 的安全托管解决方案

方案结合区政务外网的现状，充分发挥了电信云网融合和安全技术优势。实施政务外网安全防护解决方案后，区政务外网的安全通报数明显下降、端侧安全事件降低超 70%，显著提升政务外网的整体安全性、稳定性和服务能力。具体服务能力如下：

云端 : 基于电信大网威胁情报和自研见微大模型，提供高级威胁分析、研判、预警、溯源等安全服务。

利用中国电信大网 Netflow 和 PassiveDNS 数据对多源的威胁情报进行融合验证，输出精准威胁数据。具备电信骨干路由器实时流量数据，并可从实时数据中心发现威胁事件，传递到威胁情报中心发布，威胁情报中心会接入全国电信系统和安全设备的千万级日志数据，可覆盖所有威胁类型。并且通过亿级训练数据集、上亿条微调数据，对事件过滤与信息提取，实现告警压降率达到 99% 以上，精准研判安全风险事件，为安全管理人员提供了直观、准确的安全态势感知，便于及时发现并处置潜在安全风险。

边侧：面向社区 / 街道部署天翼安全网关，通过云端联动防护，特征库实时更新，为政务网接入单位提供持续的防御能力。

网关提供下一代防火墙、入侵防御、防病毒等功能，

通过云端实时监测安全风险，防止在电子政务外安全事件横向蔓延事件发生，解决边界安全防护能力不足问题。

端侧：零信任安全终端与天翼安全网关协同防护，根据身份完成访问授权，完成一体化防护闭环，消除端侧”一机两用“安全隐患。

通过 EDR 等防护软件，从事前防御、事中检测、事后闭环角度，围绕威胁全生命周期构建有效对抗、安全易闭环的终端安全防护体系。通过提供多种认证、终端环境检查、跨网隔离、违规外联检测等端到端安全防护，构建安全、易用、易管、稳定的可控可管的“一机两用”政务外网安全环境。

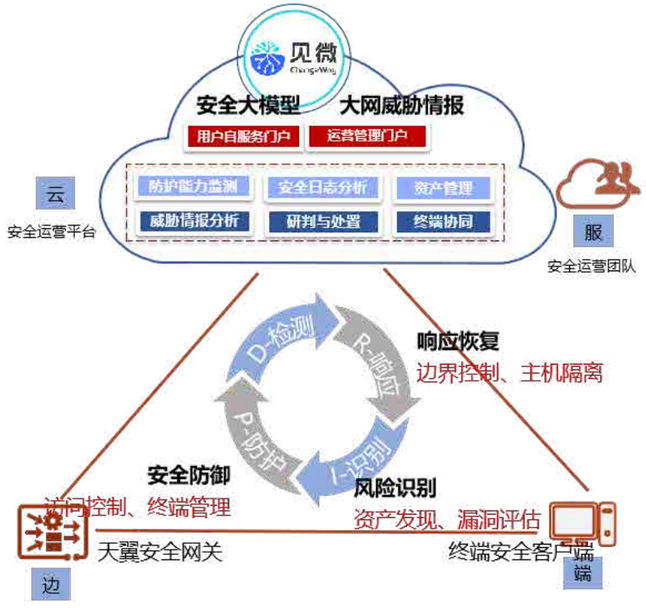
服务：一支“云端 + 属地”专业运营团队 + 一套标准安全运营流程 + 一个安全运营服务平台，提供具有运营商特色的一站式托管服务

电信打造了一个服务专家团队，通过零信任 EDR、天翼安全大脑、APT 威胁情报等安全能力的基础，运用安全数据中台（SIEM）、安全运营中台、安全能力中台（SOAR），依靠见微大模型，结合 AI 数字助手云小堤，提供资产梳理、漏洞预警、威胁研判、事件处置、服务报告等能力。通过远程托管运营、三级专家响应，分析高级威胁和可视化运维，解决日常运维人员不足的问题。

央企担当，推动政府数字化转型

中国电信股份有限公司致力于提供全方位的信息化解决方案和优质的通信服务。公司依托中国电信强大的网络资源和技术实力，专注于为政府、企业和个人用户提供网络安全、移动通信、互联网接入、云计算、大数据等一站式通信和信息化服务。

通过电子政务外网安全解决方案，保障了政务外网的整体安全性、稳定性和服务能力。通过全面防护、数据安全保障、业务连续性提升、合规性增强、用户体验优化和数字化转型推动，政务外网能够更好地服务于公众和企业，助力政府实现数字化、智能化的转型目标，共同推动数字政府建设迈向更高水平。



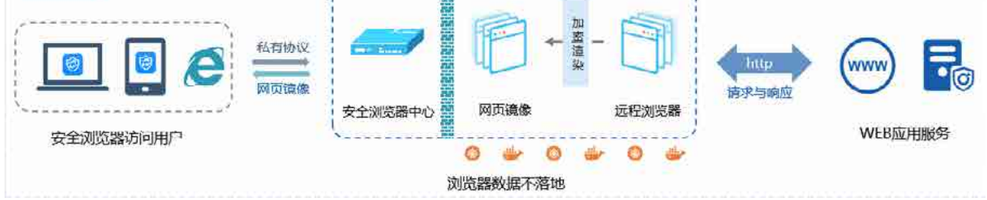
5G 网络下基于零信任浏览器的数据安全访问方案

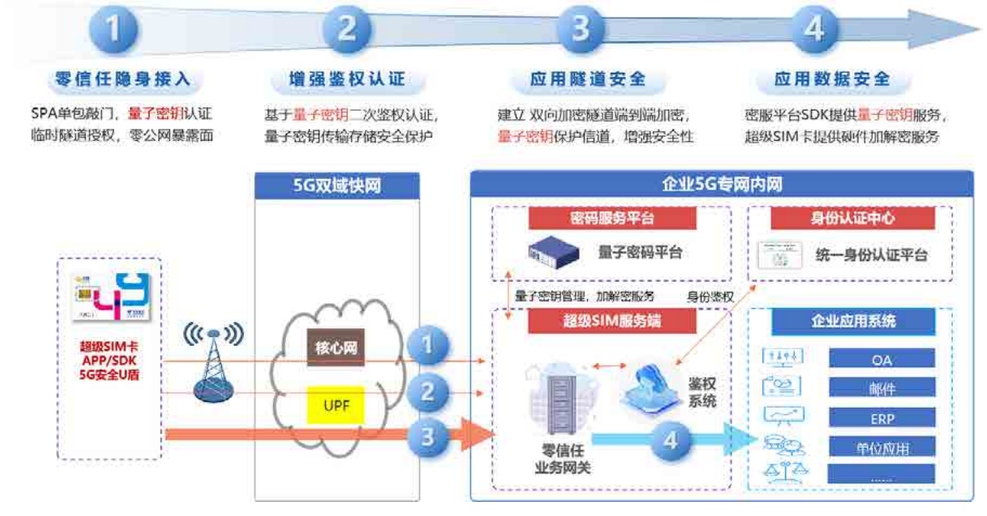
广州赛讯信息技术有限公司

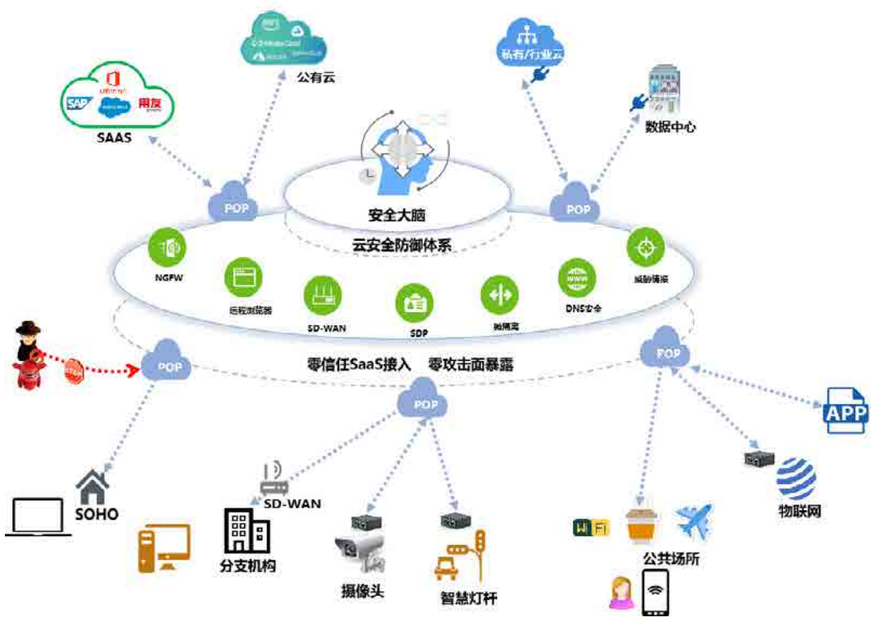
在数字化转型加速的今天，数据安全面临前所未有的挑战。广州赛讯信息技术有限公司（以下简称“赛讯”）基于 5G 网络特性与零信任安全理念，打造了一套覆盖全场景的数据安全访问方案，通过技术创新与架构融合，为政企用户构建起从网络接入到数据流转的全生命周期防护体系。

一、架构融合：5G 专网与零信任的深度协同

传统安全方案往往难以兼顾 5G 网络的高性能与安全管控需求，赛讯通过将零信任架构深度嵌入 5G 专网体系，开创了安全与效率协同发展的新模式。该方案支持有感接入与无感接入双模式，在保留 5G 网络低时延、高带宽特性的同时，实现了动态权限管控与智能风险感知。通过应用隐身技术，系统可自动隐藏非必要暴露面，结合实时行为审计功能，既保障了端到端访问的便捷性，又建立起可追溯的安全防护网。在工业互联网场景中，该体系展现出独特的适应性，既能满足生产线毫秒级响应的严苛要求，又可精准识别异常操作行为，为智能制造提供双重保障。







二、浏览器革新：数据安全的全流程护航

针对 Web 系统防护的薄弱环节，赛讯自主研发的零信任安全浏览器，通过三大核心技术重构了数据访问路径：

智能代码防护：采用动态混淆技术对网页元素进行实时伪装，隐藏关键 API 接口与敏感代码模块，有效防范注入攻击与逆向工程。

数据沙盒机制：创新 " 虚拟渲染 + 内存隔离 " 架构，确保业务数据全程仅在加密沙箱中处理，既满足数据访问需求，又彻底阻断下载外泄通道。

5G 传输优化：针对 5G 网络特性定制加密协议，在保障传输安全性的同时，显著提升大文件传输效率，为医疗影像、工业设计等场景提供无缝支持。

三、量子加密：构筑安全新防线

在加密体系设计上，赛讯突破传统密钥管理局限，构建了量子技术与零信任融合的安全生态：

动态隧道技术：通过量子密钥分发系统建立临时加密通道，每次会话采用独立密钥，结合单包敲门机制实现零公网暴露。

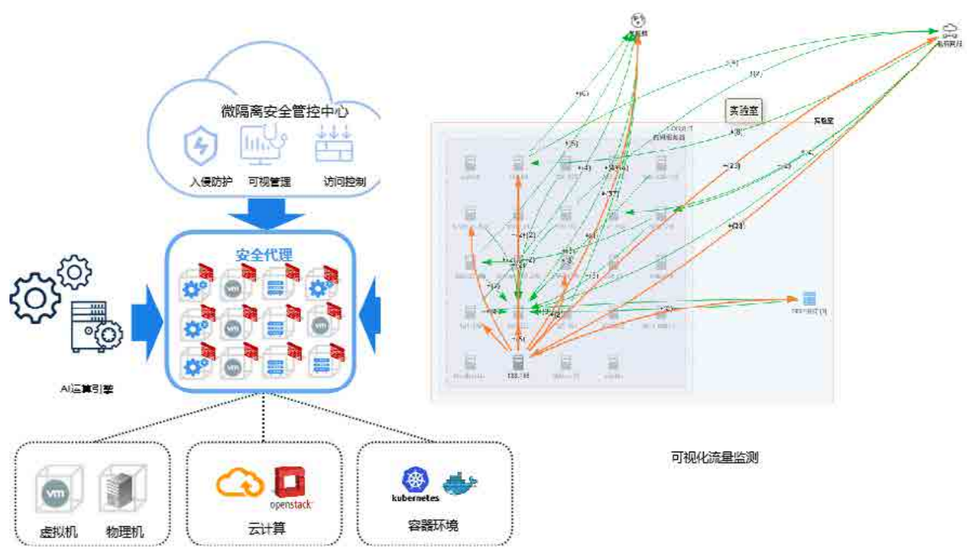
硬件级防护：集成超级 SIM 卡的国密算法模块，在移动终端形成硬件加密与量子加密的双重防护，满足等保认证要求。

自适应加密：根据网络环境智能调节加密强度，在 5G 高带宽场景下自动优化算法性能，平衡安全需求与传输效率。

四、SASE 架构：云边协同的安全服务网

基于云原生技术构建的 SASE（安全访问服务边缘）平台，实现了安全能力的分布式部署与智能化调度：

智能安全中枢：通过 AI 引擎实时分析十万级终端行为特征，建立动态威胁模型，实现攻击行为的精准预判与快速响应。



可视化流量监测

边缘防护矩阵：全国范围内部署多个边缘节点，形成百毫秒级响应的就近接入网络，大幅降低安全防护带来的时延损耗。

多云适配体系：支持主流云平台的策略同步与统一管理，通过自动化配置引擎提升跨云安全策略部署效率。

五、动态授权：智能化的权限管理体系

突破传统静态权限管理模式，赛讯构建了多维感知的动态授权系统：

环境感知引擎：整合网络负载、地理位置、设备状态等 200 余项动态参数，建立立体化风险评估模型。

微隔离管控：基于图数据库技术实现跨云业务关系可视化，支持按业务标签进行最小权限颗粒度的策略配置。

电信级融合：零信任体系与运营商 Radius 认证系统的深度对接，在万级并发场景下确保认证计费系统的精准可靠。

六、智能运维：可视化与自适应的安全治理

通过全链路测绘技术与算力网络融合，构建了新一代安全运维体系：

三维拓扑呈现：基于分布式探针实时捕获网络流量，自动生成动态可视化拓扑图，支持异常连接的快速定位与分析。

策略自优化：利用机器学习技术建立安全基线模型，可自动识别 80% 以上的策略配置冲突，实现合规检查的智能化升级。

微隔离防御：在多云环境中建立东西向流量管控机制，通过业务标签系统实现跨云资源的统一策略管理，显著提升多云环境的安全管控效率。

未来展望

广州赛讯信息技术有限公司将持续深化 5G 与零信任技术，构建 " 云 - 网 - 边 - 端 " 一体化防护体系，为数字经济发展打造自主可控的安全基座，助力用户在数字化转型浪潮中稳健前行。

基于云原生与 AI 的物联网数智安全大脑创新实践

深圳万物安全科技有限公司

摘要

物联网技术的快速发展催生了海量设备的接入，但同时也暴露了严峻的安全问题。传统的安全防护手段难以应对物联网场景下设备分散、协议私有化、攻击面复杂等挑战。深圳万物安全科技有限公司基于云原生架构与人工智能（AI）技术，创新构建了“物联网数智安全大脑”，通过多维指纹身份认证、全维度资产画像、AI 驱动威胁分析等核心技术，实现了物联网资产全生命周期安全管控。

引言

据 Gartner 预测，2022 年全球网络攻击面管理（CAASM）市场规模年增长率达 20%，物联网设备因暴露面广、防护能力弱成为攻击者的主要目标。然而，物联网设备类型繁杂、协议私有化严重、难以部署传统安全代理等问题，导致资产管理与风险防控效率低下。针对这一痛点，深圳万物安全科技有限公司（以下简称“万物安全”）提出“物联网数智安全大脑”解决方案，深度融合云原生、零信任与 AI 技术，构建了覆盖“识别 - 监测 - 防护 - 响应”的全流程安全体系。

技术架构与创新点

1. 基于云原生的分布式探测与资产识别技术

物联网设备的分散性要求安全系统具备高扩展性与实时性。万物安全采用云原生 Kubernetes 架构，支持存算分离与多机热备，系统可用性达 99.99%。通过二层分布式主动探测技术，结合 AI 驱动的协议解析引擎，可在 30 秒内完成单个 C 段网络的资产扫描，识别率超 95%。系统集成 5 万 + 物联网设备指纹库，覆盖上百种私有协议，解决了传统依赖代理（Agent）部署的局限性。

创新点：

无代理主动探测：通过流量镜像与 AI 协议逆向，10 分钟内完成设备上线与安全状态评估。

动态资产画像：整合设备属性（品牌、型号）、网络属性（IP、端口）、安全属性（漏洞、弱口令）等多维数据，构建实时更新的资产档案。

2. 零信任理念下的物联网身份认证技术

物联网设备普遍缺乏强身份标识，传统 IP/MAC 绑定方式易被仿冒。万物安全提出“多维指纹身份认证”，将设备固件版本、网络行为模式、硬件特征等静态与动态指纹结合，生成唯一身份 ID。例如，在金融场景中，系统可识别非法接入的仿冒摄像头，并联动访问控制引擎自动阻断。

创新点：

动态行为基线：AI 学习设备正常行为模式，实时检测流量异常与入侵攻击。

最小化授权：基于设备类型与业务场景动态调整访问权限，降低横向渗透风险。

3.AI 驱动的安全风险感知与响应

万物安全将大语言模型（LLM）与威胁情报结合，构建物联网安全 GPT 系统，实现威胁自动化研判。系统通过分析网络流量与日志数据，可识别 0day 漏洞利用、异常指令注入等高级攻击。例如，在交通物联网场景中，AI 引擎成功预警多起针对信号灯的近源攻击（如伪造熄火指令），响应时效提升至秒级。

创新点：

人机协同治理：AI 提供威胁线索，安全专家聚焦决策，效率提升 60%。

攻击有效性验证：模拟黑客攻击手法，主动探测设备脆弱性，生成修复建议。

应用实践与社会效益

1. 金融行业：合规与降本增效

在 TOP20 大行等案例中，系统累计发现千万级设备，处理弱口令、漏洞等风险十万例，阻断私接与仿冒事件数千余起。通过自动化资产盘点与风险处置，年节省人力成本近前往万元，并助力银行通过“护网行动”与等保 2.0 合规审查。

2. 交通系统：资产盲点治理

针对某省交通物联网前端设备分散、管理困难的问题，万物安全通过资产测绘技术（CAM）梳理出数万暗资产，识别数千余个高危漏洞，并实现设备运行状态实时监控。为智慧交通建设提供安全保障。

结论与展望

万物安全“物联网数智安全大脑”通过云原生与 AI 技术的深度融合，为物联网安全提供了创新思路。未来，团队计划进一步优化 AI 模型的多模态感知能力，并探索区块链技术在设备身份溯源中的应用。随着《网络安全法》《数据安全法》的深化实施，该方案有望在智慧城市、工业互联网等领域发挥更大价值，推动物联网安全从“被动防御”向“主动免疫”演进。

参考文献

Gartner. (2022). Top Security and Risk Management Trends.

IDC. (2023). China Video IoT Security Market Report.

中国信通院 . (2023). 物联网安全白皮书 .

万物安全 . (2023). 金融物联网安全管理解决方案 [J]. 信息安全研究 .

AiLand 数据安全岛隐私计算平台

张吉浩

武汉安恒信息科技有限公司

1 概述

数据要素可信要求

2020 年 4 月 9 日，中央第一份关于要素市场化配置的文件——《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》正式发布。《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》指出了土地、劳动力、资本、技术、数据五个要素领域改革的方向，明确了完善要素市场化配置的具体措施，加速要素市场改革，健全要素市场运行机制和组织保障，并提出要加快培育数据要素市场，包括推进政府数据开放共享，为数据要素市场化配置指明了方向。这不仅对推动数字经济高质量发展具有重大指导意义，也由此正式将数据列为与土地、劳动力、资源、技术并立的第五大生产要素。

在数据要素流通过程中，必须确保数据安全，保障交易过程是可信的。随着数字经济的发展，社会各个机数据快速积累，形成各自的“数据孤岛”。目前面临打破“数据孤岛”让多方数据融合流通时，但一旦发生数据泄漏事件，对社会、企业以及用户的危害性越大的挑战，极大地束缚了数据价值的释放。因此没有数据安全的保护，数据要素市场就会失灵，数据要素市场配置资源就不能实现对数据要素的最优配置。

数据要素有效性要求

随着数字经济发展，当今社会的数据量越来越大，但数据价值密度的高低与数据总量的大小一般成反比，数据价值密度越高，数据总量越小；数据价值密度越低，数据总量越大。任何有价值的信息的提取依托的都是海量的基础数据。大数据时代，由于不再拘泥于特定的数据收集模式，数据类型之多使数据来自多维空间，各种非结构化的数据和结构化数据混杂在一起，造成了数据质量低下。高质量的数据应具有准确性、完整性、一致性、及时性。面临如何通过算法更科学的提高数据质量、利用开发数据，将数据价值应用于数字经济领域。

政府作为一个政府治理体系的中心，管理着公共资源和数据资料，电子政务系统的建设往往是跨领域、跨地区的，各地区、各部门电子政务发展还不均衡、不充分，电子政务发展中出现各自为政、条块分割、协同治理难等问题。人们对数据流通内涵理解不一致，特别是组织单位的数据政策制定者在理解上存在差异，也导致数据流通难度大。目前我国企业生产经营数据中来自政府的仅占 7%，同时社会机构面向政府开放的数据也非常有限，企业与企业之间的数据共享更是处于冰冻状态。

2. 安全可信的数据流通方案

习近平总书记强调：“要切实保障国家数据安全，要加强关键信息基础设施安全保护，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。”发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置。面对数据流通领域的新挑战，政府、企业、行业组织需要有效配合，发挥各自优势，建立适合大数据时代要求的协同治理模式。

在遵守国家大数据安全政策框架的基础上展开顶层设计，明确“数据可用不可见，可用不可取”的总体策略，指导保障体系其他部分的开展。依据既定的安全策略，通过数据确权管理建设，明确数据流通过程中数据提供方的权利和责任，落实数据流通安全措施。根据确权管理的各项措施，在安全计算技术的支撑下，保障数据模型的安全开发。安全计算目标是采用隐私计算技术，实现“数据可用不可见，可用不可取”的理念，隐私计算技术包括：数据加密技术、多方安全计算、密文查询、密文求交、同态加密、秘密分享、区块链等技术。

自主可控的可信执行环境为数据要素流通提供环境保障，是数据要素安全的核心。大数据可信执行环境，就是依托底层大数据计算集群，配合安全调试沙箱、安全计算沙箱，身份认证和区块链合规审计等模块，结合密钥管理系统提供的统一密钥管理和加解密服务，在保障数据安全的同时，实现数据的可用不可见，可用不可取。

建设数据传输层面和应用层面的安全防护和感知能力，提供实时安全威胁分析以及对态势发展情况的预测评估，来全面描述平台整体安全情况、影响评估和态势演化。通过入侵防御系统防护外部攻击，通过日志审计及运维审计设备实时分析监控平台访问及操作行为，将流量及日志信息上送到态势感知平台进行统一的安全运营。

面向网络攻防的虚拟仿真统一平台

龙翔

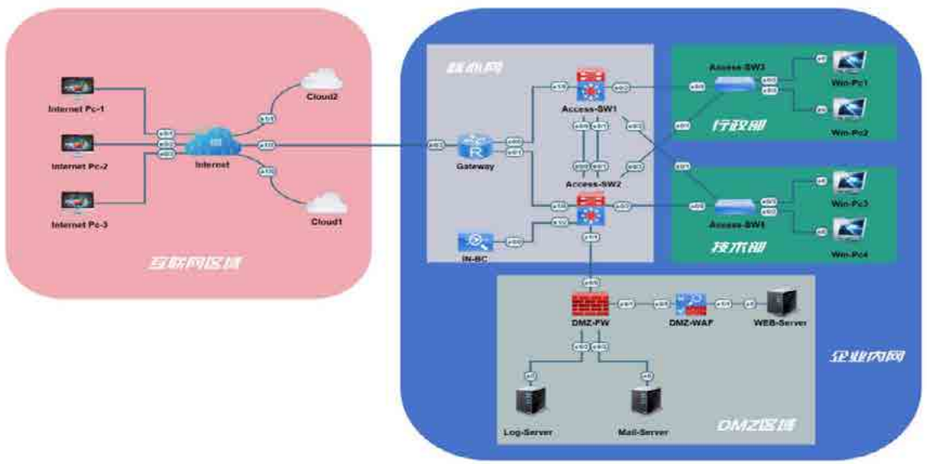
湖北生物科技职业学院

平台建设背景

网络攻防是信息安全相关从业人员经常要面对的场景，其设备众多、配置复杂、查源困难，让许多初学者学习困难。作为自研的面向网络攻防的虚拟仿真统一平台 (下文简称“华中云网”)，可在此上搭建集成多种安全设备的网络环境后，方便快捷模拟各种网络攻击与防御场景，开展流量、日志等分析，进而操作并验证成效。

应用场景说明

通过华中云网平台，部署企业的网络架构，其中逻辑划分为互联网区域和企业内网区域，在企业内网中划分了核心区域，以及 DMZ 区域。在核心区域中，扁平化设计更加方便易于管理。在 DMZ 区域中，部署了多台服务器，如网站服务器，邮件服务器和日志服务器。为了保障服务器的数据安全，还通过虚实结合技术，将现有的真实物理设备与华中云网进行联动。其中 DCFW 防火墙适用于多种网络环境，包括中小企业级市场、政府机关、大型企业、电信运营商和数据中心等机构。丰富的软件功能为网络提供不同层次及深度的安全控制以及接入管理，例如基于角色深度应用安全的访问控制、IPSec/SSL VPN、应用带宽管理、病毒过滤、内容安全等；web 应用防火墙专注于为网站及 Web 应用系统提供专业的应用层安全检测。在 Web 资产发现、漏洞评估、流量学习、威胁定位等方面，全面确保网站全天候的安全运营，提高 Web 业务系统的安全性和健壮性，抵御来自于互联网区域和内部区域的攻击，更好的保护企业数据安全。



本平台通过构建一个安全、高效且具备互动性的虚拟仿真平台，以克服传统技术供应商之间的壁垒和设备的兼容性问题，促进包括华为、华三、思科、锐捷、山石、F5 等多家厂商以及 Windows、Ubuntu、Kali、CentOS 等多种平台的整合。且在用户操作界面对所有设备进行了统一处理，用户只需从网络设备资源池中选取对应的设备即可工作。

通过本平台，网络安全相关的企业技术人员、学校师生可一比一还原真实攻防场景后进行测试、验证、对比分析。同时产品工程师可通过此平台对新产品进行方案可行性验证，给出硬件资源的最优配置，有效解决了网络资源不足、设备分散、配置复杂等问题，大大提升了网络设备使用效率，减低了组网和配置复杂度。

核心技术说明

本平台在技术方面具有显著优势，主要体现在 (1) 先进的虚拟化技术和高性能的网络仿真能力上，特别适合教学和多用户管理。平台基于 KVM 和 QEMU 技术实现了高效的硬件虚拟化。这种架构允许用户在同一物理主机上同时运行数十个虚拟设备。(2) 支持的虚实结合特性使用户能够在模拟环境中进行真实的、复杂的网络测试与实验。可以将虚拟设备的便捷部署和物理设备的性能有效结合，这样便于测试结果更贴近现实。(3) 支持图形化的操作界面，友好界面使得用户能够直观地构建和管理网络拓扑，简化设备连接与配置的过程，显著提升用户体验。(4) 支持多用户多角色使用，教师可以为不同学生分配任务，促进协作学习，满足多用户管理的需求。此外，平台还采用了 Docker 容器技术，增强了系统的可扩展性和维护性。通过平台提供的 API 接口，用户还可实现实验的自动化管理，进一步提高工作效率。综上所述，平台凭借其先进的虚拟化技术、高性能的网络仿真能力以及友好的用户界面，提升了技术应用的灵活性和实用性。

效益分析

虚拟仿真平台能够在一个平台上模拟超过千台网络安全设备，从而优化资源分配，减少资产采购和能耗成本。虚实融合后可大大提高网络物理设备的使用率，使资产动态循环利用。

该平台目前已在超过 20 所国内中高职院校中推广并得到应用，有效解决了学校在专业建设过程中面临的网络安全设备不足、系统安全环境不稳定以及网络攻防对抗案例不实用等问题。它不仅提升了学生技能培养的效率，还帮助学校实现了节能减排的目标。

通过该平台的普及使用，学生的实战技能水平得到极大的提高，毕业生的对口就业率超过 85%，且有超过 50% 的学生在国内外网络安全百强企业中就业。如图在 2023 年参加全国职业院校技能大赛高职组信息安全管理与评估赛项获一等奖。

结束语

随着数字化技术的快速发展，虚拟仿真越来越受到业内人员的关注，其使用必将更加普及和完善。特别是与 AI 结合进行安全态势感知必将为行业提供更为完备的支持和服务。

基于整车在环的车联网信息安全检测平台

左世涛　范雪俭
天融信科技集团

成果概述

基于整车在环的车联网信息安全检测平台是一套软硬件结合的自动化汽车网络与数据安全在环验证测评体系。

天融信智能网联汽车网络与数据安全测试评估通过对车联网进行系统框架分解、业务流程分析、威胁分析建模、渗透测试验证，形成以具体车载网络智能单元为对象、覆盖合规验证与渗透测试的全生命周期的标准化安全测试流程。此外，该平台采用系统虚拟化和固件仿真搭建车联网安全弹性测试环境，覆盖整车及其数据、通信、业务等应用场景，实现车联网测试场景的模拟和构建，打造车联网安全全方位在环测试评价体系，形成车联网信息安全合规验证与渗透测试一站式检测及自动化结果输出能力，为车联网网络安全和数据安全相关标准落地提供理论依据，并为主机厂、检测机构、高校等应用场景提供智能网联汽车网络安全和数据安全的综合性安全检测能力。

应用场景案例

天融信基于整车在环的车联网信息安全检测平台已经在多家主机厂、检测机构、高校等得到实际应用，为整车及零部件的网络安全、数据安全、业务安全提供了全方位的车联网安全检测与验证能力。

1）与北京某大型监督检验机构项目合作，建设北京市首个车联网信息安全检测实验室，为整车、车载总线、车端无线、车端组件、数据与业务等提供信息安全合规验证和监督检测；与公安某部联合成立车联网安全测评联合实验室，针对智能网联汽车，特别辅助驾驶、V2X、OTA 等典型业务场景的网络和数据安全能力进行测试评估，识别和解决车联网在实际应用中可能面临的网络安全挑战，提高道路车辆网络和数据安全能力；

2）《智能网联汽车网络与数据安全测试评估平台》项目获得武汉市科技局 2023 年度产业基地科技创新专项项目立项；天融信牵头编写《车联网网络安全检测技术》团体标准于 2024 年 12 月发布。车联网信息安全检测产品方案在东风汽车，襄阳达安等项目中应用。

关键技术

将新型应用场景业务适配与安全要素深度融合，形成覆盖自动驾驶（ADAS）、OTA、V2X 等典型业务场景以及全业务流程拓扑的安全测评能力；采用虚实结合、柔性接入技术，实现了整车在环的车联网网络与数据安全动态测试，解决了检测效率低、一致性差、准确率低的难题；结合大模型技术实现了标准法规快速适配、测试用例自动生成、测试用例自动优化，显著提升了测试效率、精准度；构建了自动化威胁建模引擎，实现多类别电子电器架构兼容、资产安全目标自动追溯；构建了车联网安全知识图谱，形成了多源开放、异构共享的威胁情报与安全知识库。

创新性

形成多业务场景以及全业务流程拓扑的安全测评能力；实现了整车在环的车联网网络与数据安全动态测试，解决了检测效率低、一致性差、准确率低的难题；提升测试效率、精准度；实现多类别电子电器架构兼容、资产安全目标自动追溯；形成了多源开放、异构共享的威胁情报与安全知识库。

已获得发明专利 22 项、软件著作权 4 项、安全标准制定 70 余项，可填补行业内对相关核心技术和产品紧缺的空白，解决我国在汽车安全关键技术、核心部件、产品集成能力缺失问题，补强我国智能网联汽车安全体系建设与标准法规落地实施中的核心环节，可支撑开展多层次高效用的安全标准合规验证与应用结果评价，完善安全测评体系、全面提升测评技术能力。同时，可支撑建立开放的智能网联汽车信息安全评估试验平台，减少社会资源重复投资。

可操作性及成本效益

基于整车在环的车联网信息安全检测平台和其中关键技术成果可推广至全行业，推动我国智能网联汽车信息安全产业的进一步发展，在间接经济指标效益、安全产业发展、安全人才培养、科普传播与普及等方面具有巨大的社会、经济和生态效益。

项目开展不同车型的安全防护技术研究，研发车载入侵系统。根据国内外车联网安全标准形成针对车内各控制域安全检测工具及合规方案。和该领域多家头部企业深度合作，在规模量产车型上部署，实现收入千万。

间接经济指标效益方面，除直接新增安全测评收入外，项目成果在间接经济指标效益方面有如下作用：

（1）降低安全事件带来的经济损失。推动智能终端安全分析和检测技术发展，降低智能网联汽车业务安全事件带来的经济损失，保护国家利益、用户合法权益以及汽车企业网络安全；

（2）节省国内智能网联汽车企业的研发费用。建立开放的智能网联汽车信息安全评估试验平台，可以对国内外厂商的智能网联汽车进行集中检验测试，减少社会资源重复投资带来的浪费。

网络安全工作管理平台

周伟

华中师范大学

平台建设背景

为履行网络安全主体责任，华中师范大学信息化办公室，按照网络安全等级保护制度和校园安全管理的要求，开展了网络安全工作管理平台建设工作，该平台专为教育行业打造，健全了校园网络安全防护体系，提升了高校网络安全管理水平，通过对接教育部安全管理平台以及第三方安全检测平台，以全面视角、规范流程、实现了威胁可视，责任落实到人，实现了高效应对网络安全威胁和事件的响应和处置能力。

应用场景说明

通过部署网络安全工作管理平台，建立了统一的信息资产台账，对接教育部安管平台、态势感知平台和漏洞平台，实现了安全事件处置全流程闭环管理，并建立了网络安全知识库提供培训课程。

在实际应用中，平台通过公告通知即时发布消息并确保人员周知，接收情况统计可视，加强了高校信息化办公室与各学院间的联系，使安全事件漏洞通报、限期整改、按时反馈形成完整闭环，各职能部门及院系单位能及时接收漏洞通报，按规定期限修复整改并反馈，清晰呈现事件下发状态；本平台在报平安、安全工作、年度审查、安全考核等方面发挥重要作用；如报平安功能在重保时期可及时上报异常情况；安全工作便于接收和反馈各类安全自查等工作；年度审查定期检查更新信息系统属性；安全考核体系以“安全责任制”为理念，全面评估安全工作。

通过本平台，可以提升高校网络安全管理能力，为科学决策提供支持，支持移动办公提高效率，自定义任务模板适应多种业务需求，丰富的数据报表节省人力成本，有效解决了此前面临的诸多问题，提升了整体网络安全管理水平，将网络安全工作由“被动防御，人工阻断”，升级到“主动防御，自动阻断”的新阶段，为信息化建设保驾护航。

核心技术说明

本网络安全工作管理平台基于 Hadoop 技术处理框架，实现与多类型第三方安全设备无缝对接，实时汇聚海量安全数据，本平台支持国产化架构，支持在 ARM 及 C86 等架构上运行，适配了国产操作系统及中间件，基于角色的访问控制 RBAC 模型的权限控制，可动态支持功能操作权限和数据访问权限灵活配置。

基于大数据、流计算等数字技术，实现“真正意义上”的全网安全告警降噪优化、整体安全威胁关联分析的加强，基于安全策略模型识别出来高风险事件主体，可实现基于时间的半自动、全自动化的安全响应。通过多维度安全策略建模落地 ATT&ACK 攻击行为监测框架累计 100+ 策略模型，实现攻击源在全网范围内的攻击行为链路关联、回溯。

平台支持多种协议渠道采集，如 UDP、kafka、文件等，围绕数据使用过程，提供了全栈式的数据集成功能，将原始杂乱数据提炼成各种安全数据模型，自由对接国内外厂商各种安全产品、设备、应用等数据，不存在围绕某个生态只集成所属生态内产品的情况。

效益分析

该平台具有较高的可操作性，其功能模块设计清晰，操作流程简便，如安全事件处理流程明确，各学院单位能轻松接收通报并按流程完成整改反馈。平台支持多种便捷操作方式，如报平安功能可与企业微信对接实现手机报平安，方便人员使用。

在成本效益方面，从整体上提升了单位的安全防护水平，从而使得高校和组织的成本效益最大化，降低总拥有成本（TCO），提升安全设施的投资回报率（ROI）；前期投入主要集中于平台建设及设备对接等，相对传统安全管理方式，无需大量额外硬件设备购置，降低了硬件成本。平台上线后，通过优化安全任务流程、提高运维效率，减少了人力投入成本。例如，自动化的漏洞管理和安全事件处理流程，节省了人工排查和处理的时间与精力。

同时，有效降低安全事件发生概率，规避了因安全事件带来的绩效损失、经济赔偿等风险，从长期看产生了显著的安全效益。且丰富的数据报表功能有助于精准定位问题，进一步优化资源配置，提高整体网络安全管理的投入产出比，为高校网络安全管理提供了高性价比的解决方案。

结束语

在数字化高速发展之路上，该平台进一步完善高校的网络安全建设体系，主要功能符合教育行业的实际运用现状何要求，如资产管理、漏洞管理、安全事件全流程处理、各类安全任务执行、备案登记管理及安全知识库等功能实现了安全管理工作的日常化管理，事件状态清晰可见，便于实时掌控。

武汉市网络安全协会服务指南

一 移动应用安全公益检测服务

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

二 网络安全等级保护测评

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

三 网络安全保险服务

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

四 网络安全相关标准制定服务

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

五 资质认证

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

六 人才服务

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

七 咨询服务

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

八 网络安全宣传与会务服务

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

武汉市网络安全协会入会指南

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

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

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

入会基本条件

依据我会《章程》规定，我会会员分为单位会员和个人会员，入会基本条件如下：

一、在武汉市注册的企事业法人单位、具有武汉市户籍或长期居住的专业人士。

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

二、从事以下某项或多项领域的单位和专业人士：

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

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

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

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

5. 应用安全：应用服务安全、应用服务安全支持；

6. 数据安全：数据平台安全（安全数据库、数据库安全部件等）、备份与恢复；

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

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

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

10. 在网络安全和信息化产业链上下游关系紧密的有关机构和专业人士。

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

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

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

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

入会流程

一 申请人填写《武汉市网络安全协会入会申请表》提交协会；
二 协会进行入会资格审核；
三 符合入会条件，协会核发《入会通知书》；
四 申请单位或个人按要求提交纸质版材料 1 份，并按规定标准缴纳会费；
五 会籍资料存档，协会颁发会员证书或标牌并公示；

入会联系人：张玉萍　　联系电话：027—85519110　　http://www.whcsa.org.cn