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 Cyber 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
电话：027—85519110　　网址：www.whcsa.org.cn　　邮箱 :hz@whcsa.org.cn

声明：本通讯内容属内部资料，原创内容未经本单位同意不得转载。
此资料为电子版样本，仅供部分会员单位审阅，内容如有遗漏错误请及时与我会联系反馈，我们将在正式版本更正。

武汉网络安全
2026年第1期　总第7期

武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2026年第1期　总第7期

内部资料　电子样本

◎ 政策速递 /04P
国家网信办、工业和信息化部、公安部
联合公布《网络数据安全风险评估办法》

◎ 党政引领 /22P
喜报！武汉市网络安全协会党支部
荣获“全市先进基层党组织”称号

◎ 江城安讯 /28P
武汉新增全国唯一网安类本科高校，今秋招生

◎ 协会动态/38P
武汉市网络安全协会第二届理事会
第七次会议顺利召开

◎ 教育数智化安全治理专栏/62P
"数智问道 智护校园安澜"
教育数智化安全治理主题活动圆满举行

◎ 教育行业数据安全案例集/66P



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

武汉市网络安全协会简介

INTRODUCTION TO WUHAN 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全市性、专业性、非营利性组织。

我会党支部做实做优“两新”组织党建工作，以党建引领赋能网络安全产业发展，被中共武汉市委授予“全市先进基层党组织”荣誉称号。我会是民政部门认定的AAAA级社会组织;是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，中国网络空间安全协会智能网联安全专业委员会发起单位,国家网络安全人才与创新基地产业联盟运营单位，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,入选湖北省第一批优质团体标准制定主体重点培育名单；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”；是武汉市职称改革领导小组办公室授权的全市职称评审行业主管单位；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、民办高校工作委员会、人工智能专业委员会和医疗卫生与健康分会；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、重庆、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。

我会各项工作长期得到各级官方媒体的支持和关注，新华网、人民网、光明网、学习强国、中国新闻网、湖北日报（荆楚网）、长江日报（长江网）相继报道我会工作动态和成果。

我会的宗旨：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

作为武汉网络安全人才培养的重要阵地与平安校园建设的关键防线，民办高校的网安事业始终牵动着行业发展的脉搏。自2024年经武汉市网络安全协会批复成立，民办高校工作委员会已与22所成员高校并肩走过两年深耕之路，从最初的凝心聚力起航，到如今形成本科与职业院校全覆盖的协同格局，我们始终以“守护校园网络、培育网安人才”为初心，走出了一条独具特色的共建之路。

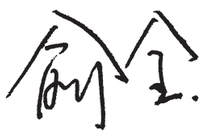
两年来，我们坚持党建与业务同频共振，将党的网络强国战略转化为校际协作的具体行动；创新“1+2+N”工作模式，让“网络安全第一课”走进近万名新生课堂，让高仿真攻防演练锤炼各校应急处置硬功，让校际教学资源库打破院校壁垒。在省教育厅组织的攻防演练中，成员高校排名稳步提升，全年实现重大网络安全事故零发生，交出了一份扎实的年度答卷。

面对后续工作，武汉市民办高校工作委员会将持续推进民办高校网络安全工作准则落地实施，以标准化建设引领行业规范发展。我们将把准则要求贯穿于校园防护、人才培养、校际协作的全过程，着力补齐发展短板，破解共性难题。

围绕这一目标，工委会将继续秉持“共建、共享、共防”理念，全力推动专项支持计划落地，深化校企协三方联动，搭建校际互助帮扶平台。我们将以更坚定的决心筑牢校园网络防线，以更开放的姿态整合各方资源，努力让每一所民办高校都成为网安人才的摇篮、数字安全的堡垒，为武汉网络安全事业高质量发展注入源源不断的民办力量。



武汉市网络安全协会民办高校工作委员会主任
武汉设计工程学院网络中心主任



目 录

CATALOGUE

政策速递

04 国家网信办、工业和信息化部、公安部联合公布《网络数据安全风险评估办法》

07 国家网信办、公安部就《大型网络平台个人信息保护规定（征求意见稿）》公开征求意见

11 关于印发《可能影响未成年人身心健康的网络信息分类办法》的通知

14 关于印发《网络安全标识管理办法》的通知

17 市人民政府关于印发武汉市支持人工智能OPC创新发展若干措施的通知

党建引领

22 喜报！武汉市网络安全协会党支部荣获“武汉市先进基层党组织”称号

24 湖北党员生活杂志社、常青街道党工委莅临我会指导党建工作

25 武汉市网络安全协会党支部与市计量标准质量研究院第六支部开展联学共建主题党日活动

26 市公安局网安支队六大队与市网络安全协会联合开展“迎七一·强党性·保安全”主题党日活动

27 武汉市网络安全协会党支部组织集中收看中国共产党成立105周年大会

江城安讯

28 武汉新增全国唯一网安类本科高校，今秋招生

32 全国唯一！首次开放

33 2026年“黄鹤杯”网络安全人才创新大赛启幕

34 “中国网谷”科创政策矩阵发布
大型人工智能企业设总部最高支持2亿元

35 武汉大学召开2026年度网络安全工作会议

36 当“小龙虾”游入“中国网谷”：折射网安信创产业新生态

协会动态

38 武汉市网络安全协会第二届理事会第七次会议顺利召开

40 武汉市网络安全协会2025年终团建交流活动圆满举办

41 我会收到中国网络空间安全协会感谢信

42 我会协办的“湖北省‘51020’先进制造业集群产业生态之新型信息网络产业链专场活动”在汉举办

44 武汉市网络安全协会受邀为湖北交投高创监理公司专题培训授课

45 武汉市网络安全协会组织召开网络安全“双安认定”团体标准编制推进会

46 武汉市网络安全协会走访慰问会员单位并致以新春感谢

47 武网安协赴汉阳市政汇科智创开展工程行业网络安全合规专题培训

48 武汉市网络安全协会走进中国铁建港航局集团有限公司第六工程分公司 筑牢工程领域网络安全防线

51 武汉市网络安全协会第二届理事会第四次会长办公会顺利召开

52 武网安协召开《网络安全企业认定规范》《网络安全产品和服务认定规范》团体标准编制委员会第二次全体会议

53 “学子聚汉”工程计算机类专场招聘活动顺利举办

55 喜获省级认证！我会知识产权人才队伍再壮大服务能力迈上新台阶

56 默安科技：以AI驱动主动防御 筑牢数字安全坚实屏障

58 赋能产业 · 精准惠企
武汉科创政策宣贯助力网安与AI产业高质量发展

60 精准赋能专技人才 助力产业提质升级

61 深化跨界协同共筑产业安全一
武汉市网络安全协会走访武汉市新能源汽车产业协会

教育数智化安全治理专栏

63 “数智问道 智护校园安澜”教育数智化安全治理主题活动圆满举行

67 中国地质大学校园数据安全综合治理创新实践项

69 华中农业大学教育数据全生命周期安全治理与合规项目
——华中农业大学

72 某教育数据中心敏感数据安全管控与防护项目
——武汉通达数据科技有限公司

74 教育行业考试报名系统数据安全风险评估与整改项目
——武汉安域信息安全技术有限公司

77 某高校量子科技创新及校园量子加密通信网搭建项目
——中国电信股份有限公司武汉分公司

80 某财大智慧校园数据安全综合治理与防护项目
——杭州安恒信息技术股份有限公司

82 湖北国土职院智慧校园数据共享与安全防护项目
——湖北国土资源职业技术学院

84 湖北大学云网安运管平台建设项目
——湖北大学

86 开放式云化校园网络
——星融元

88 教育行业数据安全典型案例
——湖北某省属“双一流”高校

90 基于信创架构的数据安全与云化升级项目
——某省属重点高等院校

92 高校基于“态势感知+数据中心防火墙”的内网横向攻击隔离与数据安全治理项目
——湖北大学知行学院

94 人脸数据安全中台教育数据安全案例
——武汉学院

96 面向数智化校园基础设施解决方案
——宏杉科技

国家网信办、工业和信息化部、公安部联合公布《网络数据安全风险评估办法》

国家互联网信息办公室

中华人民共和国工业和信息化部

中华人民共和国公安部

令

《网络数据安全风险评估办法》已经2026年6月1日国家互联网信息办公室2026年第12次室务会会议审议通过，并经中华人民共和国工业和信息化部、中华人民共和国公安部同意，现予公布，自2026年8月20日起施行。

国家互联网信息办公室主任　庄荣文

工业和信息化部部长　李乐成

公安部部长　王小洪

2026年6月18日

网络数据安全风险评估办法

第一章　总　则

第一条　为了规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》、《中华人民共和国网络安全法》、《网络数据安全管理条例》等法律法规，制定本办法。

第二条　在中华人民共和国境内开展网络数据安全风险评估，应当遵守本办法。

本办法所称网络数据安全风险评估（以下简称风险评估），是指对网络数据和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动。

第三条　在国家数据安全工作协调机制指导下，国家网信部门会同国务院电信、公安等有关部门建立网络数据安全风险评估专项工作机制，指导、监督风险评估工作。

第四条　有关主管部门应当按照谁管业务、谁管业务数据、谁管数据安全的原则，定期组织开展本行业、本领域风险评估，根据工作需要对本行业、本领域处理重要数据的网络数据处理者（以下简称重要数据处理者）开展风险评估情况进行检查，并于每年1月底前将年度风险评估检查计划报送国家网信部门。国家网信部门通过国家数据安全工作协调机制将计划与国务院电信、公安、国家安全等有关部门共享并进行协调，避免不必要的检查和交叉重复检查。

有关主管部门开展检查不得向被检查的重要数据处理者收取费用。

第五条　重要数据处理者应当每年度开展风险评估。

重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应当及时对发生变化及其影响的部分开展风险评估。

鼓励处理一般数据的网络数据处理者（以下简称一般数据处理者）至少每3年开展一次风险评估。

第六条　风险评估工作应当按照《中华人民共和国数据安全法》、《网络数据安全管理条例》有关要求，参照数据安全风险评估有关国家标准开展。有关主管部门对本行业、本领域风险评估工作另有规定的，从其规定。

第七条　网络数据处理者可以自行或者委托第三方评估机构（以下简称评估机构）开展风险评估。

网络数据处理者自行开展风险评估，应当指定专人负责。网络数据处理者委托评估机构开展风险评估，应当通过订立合同或者其他具有法律效力的文件等方式明确双方的权利、义务等。

第八条　鼓励相关评估机构通过认证。评估机构的认证按照《中华人民共和国认证认可条例》的有关规定执行。

第九条　在国家数据安全工作协调机制指导下，国家网信部门和国务院电信、公安等有关部门积极促进网络数据安全风险评估服务的发展，培育评估机构。

第十条　评估机构开展风险评估应当遵守法律法规，公正客观地作出风险判断，并对所出具的风险评估报告真实性、有效性、完整性负责。

第十一条　评估机构不得转委托其他机构开展风险评估。

第十二条　同一评估机构及其关联机构不得连续3次以上对同一网络数据处理者开展年度风险评估。

第十三条　评估机构在风险评估过程中发现网络数据处理活动存在重大数据安全风险的，应当及时通知网络数据处理者。

第十四条　评估机构及其工作人员应当对在风险评估过不得泄露或者非法向他人提供，在风险评估结束后及时删除或者按照合同约定妥善处置相关信息。

第十五条　重要数据处理者开展年度风险评估，应当依法按照有关主管部门规定编制风险评估报告。有关主管部门对风险评估报告没有规定的，可以参照数据安全风险评估有关国家标准编制风险评估报告。风险评估报告至少保存3年。

一般数据处理者可以参照前款要求编制风险评估报告。

第十六条　重要数据处理者应当在年度风险评估完成后的20个工作日内按照有关主管部门要求向其报送风险评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。

有关主管部门应当公开风险评估报告报送渠道和联系方式，及时接收重要数据处理者报送的风险评估报告，自收到风险评估报告之日起的10个工作日内将报告通报同级网信部门。国家网信部门汇总相关报告，并与国务院电信、公安、国家安全等有关部门共享。

省级以上网信部门、电信主管部门、公安机关、国家安全机关和其他有关部门可以对重要数据处理者的风险评估报告真实性、准确性进行检查核验，重要数据处理者应当配合开展检查核验。

第十七条　省级以上网信部门、电信主管部门、公安机关和其他有关部门在风险评估报告核验、监督检查等工作中发现网络数据处理者有以下情形之一的，可以要求其委托通过认证的评估机构开展风险评估：

（一）网络数据处理活动存在较大安全风险，可能危害国家安全、公共利益的；

（二）发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的；

对同一网络数据安全事件或者风险，不得重复要求网络

数据处理者委托评估机构开展风险评估。

第十八条　网络数据处理者按照有关部门要求委托评估机构开展风险评估的，应当履行下列义务：

（一）为评估机构开展风险评估提供必要支持，包括为风险评估人员提供必要的访问网络数据设施、网络数据、系统及操作日志记录权限等；

（二）在限定时间内完成风险评估，情况复杂的，报有关部门批准后可以适当延长；

（三）在完成风险评估后将评估机构出具的风险评估报告报送有关部门，风险评估报告应当由评估机构主要负责人、风险评估负责人签字并加盖机构公章；

（四）按照有关部门要求对风险评估中发现的问题进行整改，在整改完成后15个工作日内，向有关部门报送整改情况报告。

网络数据处理者不得以任何方式要求或者示意评估机构出具不实或者不当的风险评估报告。

第十九条　有关部门在组织开展风险评估中发现重要数据处理者的重要数据处理活动可能危害国家安全、公共利益的，应当依据职责责令重要数据处理者进行整改；对拒不整改或者未达到整改要求的重要数据处理者，可以采取要求其停止处理重要数据等措施。

第二十条　有关主管部门应当加强风险信息共享和协同处置，及时处置风险评估中发现的安全风险和问题，并按照有关规定及时报告。

（二）在限定时间内完成风险评估，情况复杂的，报有关部门批准后可以适当延长；

（三）在完成风险评估后将评估机构出具的风险评估报告报送有关部门，风险评估报告应当由评估机构主要负责人、风险评估负责人签字并加盖机构公章；

（四）按照有关部门要求对风险评估中发现的问题进行整改，在整改完成后15个工作日内，向有关部门报送整改情况报告。

网络数据处理者不得以任何方式要求或者示意评估机构出具不实或者不当的风险评估报告。

第十九条　有关部门在组织开展风险评估中发现重要数据处理者的重要数据处理活动可能危害国家安全、公共利益的，应当依据职责责令重要数据处理者进行整改；对拒不整改或者未达到整改要求的重要数据处理者，可以采取要求其停止处理重要数据等措施。

第二十条　有关主管部门应当加强风险信息共享和协同处置，及时处置风险评估中发现的安全风险和问题，并按照有关规定及时报告。

第二十一条　任何组织、个人有权对风险评估中的违法活动向有关部门进行投诉、举报，收到投诉、举报的部门应当依法及时处理。

第二十二条　省级以上网信部门、电信主管部门、公安机关、国家安全机关或者其他有关部门发现网络数据处理者未按规定开展风险评估的，应当依据《中华人民共和国数据安全法》、《网络数据安全管理条例》等有关法律、行政法规予以处理。

发现评估机构违反本办法开展风险评估的，有关部门应当依法予以处理。

第二十三条　处理核心数据的网络数据处理者的风险评估，按照国家有关规定执行。

涉及重要数据加密等技术措施的，应当按照国家密码相关法律、行政法规要求开展商用密码应用安全性评估。

第二十四条　开展涉及国家秘密、工作秘密的风险评估活动，按照《中华人民共和国保守国家秘密法》等法律、行政法规及国家保密规定执行。

第二十五条　本办法自2026年8月20日起施行。

国家网信办、公安部就《大型网络平台个人信息保护规定（征求意见稿）》公开征求意见

为规范大型网络平台个人信息处理活动，保护个人信息合法权益，促进平台经济健康发展，根据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室、公安部起草了《大型网络平台个人信息保护规定（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

1.登录中国网信网（www.cac.gov.cn），进入首页“网信要闻”查看文稿。

2.登录公安部官网（www.mps.gov.cn），进入首页“调查征集”查看文稿。

3.通过电子邮件方式发送至：shujuju@cac.gov.cn。

4.通过信函方式将意见寄至：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“大型网络平台个人信息保护规定征求意见”。

意见反馈截止时间为2025年12月22日。

附件：《大型网络平台个人信息保护规定（征求意见稿）》

国家互联网信息办公室

公安部

2025年11月22日

大型网络平台个人信息保护规定（征求意见稿）

第一条 为规范大型网络平台个人信息处理活动，保护个人信息合法权益，促进个人信息依法合理利用，根据《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《网络数据安全管理条例》等法律法规，制定本规定。

第二条　在中华人民共和国境内建设、运营的大型网络平台的个人信息保护，适用本规定。法律、行政法规另有规定的，从其规定。

第三条 国家网信部门会同国务院公安部门等有关部门制定发布大型网络平台目录并动态更新。对大型网络平台的认定，主要考虑以下因素：

（一）注册用户5000万以上或者月活跃用户1000万以上；

（二）提供重要网络服务或者经营范围涵盖多个类型业务；

（三）掌握处理的数据一旦被泄露、篡改、损毁，对国家安全、经济运行、国计民生等具有重要影响；

（四）国家网信部门、国务院公安部门规定的其他情形。

第四条　提供大型网络平台服务的网络数据处理者（以下简称大型网络平台服务提供者）开展个人信息处理活动，应当遵循合法、正当、必要和诚信原则，遵守法律、法规，遵守社会公德和伦理，对所处理的个人信息安全承担主体责任，严格保护敏感个人信息和未成年人个人信息，承担社会责任，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。

第五条　大型网络平台服务提供者应当按照法律法规有关规定指定个人信息保护负责人，并公开个人信息保护负责人的联系方式。

个人信息保护负责人应当由大型网络平台服务提供者管理层成员担任，具有中华人民共和国国籍，无境外永久居留权或者长期居留许可，具备个人信息保护专业知识且从事相关工作5年以上。个人信息保护负责人可以由网络数据安全负责人兼任。

个人信息保护负责人应当履行下列职责：

（一）指导大型网络平台合规开展个人信息处理活动，落实国家网信部门、国务院公安部门和有关主管部门的个人信息保护监管要求，配合有关部门开展个人信息保护监督检查；

（二）参与大型网络平台个人信息处理事项相关决策，并对个人信息处理事项具有否决权；

（三）负责对个人信息处理活动以及采取的保护措施等进行监督，发现大型网络平台个人信息处理活动存在较大安全风险或者存在违法违规情形的，应当立即采取措施，并向国家网信部门和有关主管部门报告，涉嫌违法犯罪的应当向公安机关报案；

（四）组织制定专门的未成年人个人信息处理规则。

个人信息保护负责人可以直接向国家网信部门、有关主管部门报告大型网络平台服务提供者的个人信息保护有关情况。

第六条　大型网络平台服务提供者应当明确个人信息保护工作机构，在个人信息保护负责人领导下开展个人信息保护相关工作，包括但不限于：

（一）制定实施内部个人信息保护管理制度、操作规程以及个人信息安全事件应急预案，合理确定个人信息处理的操作权限，对大型网络平台的个人信息处理活动进行安全管理；

（二）组织开展个人信息安全风险监测、风险评估、合规审计、影响评估、应急演练、宣传教育培训等活动，及时处置个人信息安全风险和事件；

（三）明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务，并对其个人信息处理活动和履行个人信息保护义务情况进行监督；

（四）明确专人负责未成年人个人信息保护工作；

（五）受理并处理个人信息保护投诉、举报；

（六）每年编制发布大型网络平台服务提供者个人信息保护社会责任报告。鼓励大型网络平台服务提供者设立专门的个人信息保护工作机构。

第七条 大型网络平台服务提供者应当为个人信息保护负责人、个人信息保护工作机构履行职责提供必要支持。

第八条 大型网络平台服务提供者应当及时向国家网信部门报送下列信息：

（一）个人信息保护负责人基本信息；

（二）个人信息保护工作机构基本信息；

（三）保障个人信息保护负责人和个人信息保护工作机构履职的措施。

个人信息保护负责人、个人信息保护工作机构等发生变化的，大型网络平台服务提供者应当在20个工作日内报送变更信息。

国家网信部门将大型网络平台服务提供者信息向国务院公安部门和有关主管部门共享。

第九条　大型网络平台服务提供者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在境内。确需向境外提供的，应当符合国家数据出境安全管理有关规定。

大型网络平台服务提供者应当按照国家有关规定，健全个人信息出境安全相关技术和管理措施，及时防范、处置个人信息违法违规出境安全风险和威胁。

第十条　大型网络平台服务提供者应当将在中华人民共和国境内运营中收集和产生的个人信息存储在符合下列条件的数据中心：

（一）设立在中华人民共和国境内；

（二）主要负责人具有中华人民共和国国籍，无境外永久居留权或者长期居留许可；

（三）安全性符合国家有关标准要求。

第十一条　数据中心应当协助大型网络平台服务提供者履行个人信息保护义务，包括但不限于：

（一）建立健全内部个人信息管理制度和操作规程；

（二）发现系统、网络产品和服务等存在影响大型网络平台服务提供者履行个人信息保护义务的安全缺陷、漏洞等风险的，应当立即采取补救措施，按照规定向有关主管部门报告，并通报大型网络平台服务提供者个人信息保护负责人；

（三）发生个人信息安全事件时，应当立即通报大型网络平台服务提供者个人信息保护负责人，及时启动应急处置预案，采取措施防止危害扩大，消除安全隐患，并按照规定向国家网信部门、有关主管部门报告；

（四）及时执行国家网信部门、国务院公安部门和有关主管部门个人信息安全保护有关要求。

第十二条　大型网络平台服务提供者委托符合本规定第十条要求的第三方数据中心存储个人信息的，应当与其签订合同，约定存储地点、规模、种类等，明确履行本规定第十一条按要求和下列职责：

（一）严格依照法律法规的规定和合同约定，履行个人信息保护义务，提供安全、稳定、持续的服务，并接受大型网络平台服务提供者个人信息保护负责人、个人信息保护监督委员会等的监督；

（二）为大型网络平台服务提供者处理个人信息提供便利措施；

（三）协助大型网络平台服务提供者对个人信息处理活动进行安全管理。

第十三条 大型网络平台服务提供者应当向国家网信部门等有关部门报送存储个人信息的数据中心的基本信息，包括管理团队和管理架构、内部个人信息保护管理制度、采取的安全措施、与第三方数据中心签署的合同文本等。上述信息发生变化的，应当自变化之日起10个工作日内报送变更信息。

第十四条　大型网络平台服务提供者应当为个人行使查阅、复制、更正、补充、删除、限制处理其个人信息，或者注销账号、撤回同意等权利提供便捷的方法和途径。

个人请求将其个人信息转移至其指定的个人信息处理者的，大型网络平台服务提供者应当在接到个人请求后30个工作日内将个人信息通过通用、机器可读的格式进行转移，并以邮件、电话、短信等方式告知个人处理结果，不符合法律、行政法规规定条件的，应当向个人说明原因。因请求数量、操作复杂等原因需要延长处理期限的，应当向个人说明原因。因请求数量、操作复杂等原因需要延长处理期限的，应当向个人说明延期原因，可以在合理、必要的情况下再延长30个工作日。法律、行政法规、部门规章另有规定的，从其规定。

支持大型网络平台服务提供者通过应用程序接口或者其他标准化技术方式提供转移途径，采取身份验证、加密传输等安全措施保障个人信息转移安全。

个人重复转移个人信息的，大型网络平台服务提供者可

以根据转移个人信息的成本收取必要费用。

第十五条 大型网络平台服务提供者应当按照国家有关规定自行或者委托第三方专业机构开展个人信息保护合规审计、风险评估等活动，并对发现的问题进行整改。鼓励大型网络平台服务提供者优先选择通过认证的第三方专业机构。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。

第十六条 受大型网络平台服务提供者委托开展个人信息保护合规审计、风险评估等活动的第三方专业机构，应当注册在中华人民共和国境内，发现大型网络平台服务提供者的个人信息处理活动存在较大安全风险或者存在违法违规情形的，可以直接向国家网信部门和有关主管部门报告；涉嫌违法犯罪的应当向公安机关报案。

第十七条 大型网络平台服务提供者有以下情形之一的，国家网信部门、国务院公安部门和有关主管部门可以要求其委托第三方专业机构对其个人信息处理活动开展合规审计、风险评估等活动：

（一）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情形的；

（二）多次出现个人信息违规出境等违法违规情形的；

（三）个人信息处理活动可能侵害众多个人权益的；

（四）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；

（五）法律法规和有关主管部门规定的其他情形。

大型网络平台服务提供者应当配合第三方专业机构履行职责，为第三方专业机构开展工作提供必要保障，包括为第三方专业机构指定人员提供必要的访问大型网络平台网络数据设施、系统及操作日志记录权限等。

发现大型网络平台服务提供者无能力保障个人信息安全的，国家网信部门、国务院公安部门和有关主管部门可以要求大型网络平台服务提供者通过签订合同等方式将个人信息存储在符合本规定要求的第三方数据中心。

第十八条 鼓励大型网络平台服务提供者应用国家网络身份认证公共服务、使用数据标签标识技术、通过个人信息保护认证等，提高个人信息保护水平。

第十九条 鼓励大型网络平台服务提供者开展个人信息保护相关技术、产品、服务创新，积极参与个人信息保护相关国际标准和规则制定，推动与其他国家、地区之间的个人信息保护规则、标准协调互认。

第二十条 任何组织和个人有权对大型网络平台服务提供者、第三方数据中心违反本规定的活动，向履行个人信息保护职责的部门进行投诉、举报。收到投诉、举报的部门应当在15个工作日内依法处理，并将处理结果告知投诉、举报人。

履行个人信息保护职责的部门应当加强信息共享，协同开展相关工作。

第二十一条 网信部门、公安机关和有关主管部门发现大型网络平台服务提供者、第三方专业机构或者数据中心未履行个人信息保护责任的，依法追究责任；构成犯罪的，依法追究刑事责任。

第二十二条 国家网信部门、国务院公安部门和有关主管部门、第三方数据中心、第三方专业机构的工作人员应当对工作过程中知悉的个人隐私、个人信息、商业秘密、保密商务信息等依法予以保密，不得泄露或者非法向他人提供。

第二十三条 开展涉及国家秘密、工作秘密的个人信息处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

大型网络平台应当落实网络安全等级保护有关要求，属于关键信息基础设施的大型网络平台，还应当遵守国家关于关键信息基础设施安全的有关规定。

第二十四条 本规定自2026年7月1日起施行。

关于印发《可能影响未成年人身心健康的网络信息分类办法》的通知

国信办通字〔2025〕5号

各省、自治区、直辖市互联网信息办公室、新闻出版局、电影主管部门、教育厅（局）、通信管理局、公安厅（局）、文化和旅游厅（局）、广播电视局，新疆生产建设兵团互联网信息办公室、新闻出版局、电影主管部门、教育局、公安局、文化体育广电和旅游局：

现将《可能影响未成年人身心健康的网络信息分类办法》印发给你们，自2026年3月1日起施行，请认真贯彻执行。

国家互联网信息办公室

国家新闻出版署

国家电影局

教育部

工业和信息化部

公安部

文化和旅游部

国家广播电视总局

2025年12月26日

可能影响未成年人身心健康的网络信息分类办法

第一条 为了营造有利于未成年人身心健康的网络环境，进一步明确可能影响未成年人身心健康的网络信息的具体种类、范围、判断标准和提示办法，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》、《未成年人网络保护条例》、《互联网信息服务管理办法》、《网络信息内容生态治理规定》、《网络暴力信息

治理规定》等法律法规规定，制定本办法。

第二条　本办法所称的可能影响未成年人身心健康的网络信息，是指除法律法规规定的含有危害未成年人身心健康内容的违法信息外，通过互联网发布传播的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、养成不良嗜好等的信息。

第三条　可能引发或者诱导未成年人模仿或者实施不良行为的信息包括但不限于：

（一）带有性暗示、性挑逗等易使人产生性联想的；

（二）存在指责嘲讽、贬低歧视等涉网络暴力不良信息的；

（三）煽动人群歧视、地域歧视、对立冲突等行为的；

（四）通过刻意刺激、恶意引导等方式，引发未成年人产生过度强烈或者持久的愤怒、恐惧、抑郁等极端情绪的；

（五）存在不安全驾驶等危险动作，诱导模仿高风险行为、进入危险区域等可能损害身体健康行为的；

（六）通过谐音梗、缩写词、拆解字、图文结合等形式传播不良网络用语的；

（七）宣扬未成年人抽烟（含电子烟）、饮酒、暴饮暴食、文身、不合理使用或者滥用药物等不良生活方式的；

（八）宣扬代写代抄、抄袭作弊、逃学旷课、学生欺凌等违校纪校规行为的；

（九）诱导未成年人盲目追星、参与非理性极端“饭圈”行为的；

（十）诱导未成年人进行充值、打赏等非理性消费行为的；

（十一）教授未成年人制作具有伤害性的创意手工的；

（十二）向未成年人提供或者寻求陪玩陪聊、代练代打等服务的；

（十三）其他可能引发或者诱导未成年人模仿或者实施不良行为的。

第四条　可能对未成年人价值观造成负面影响的信息包括但不限于：

（一）宣扬漠视生命、自我贬损等观念的；

（二）宣扬奢靡享乐、炫富拜金、消极颓废等不良价值观的；

（三）宣扬畸形审美、低俗恶俗文化的；

（四）宣扬荒诞离奇、危言耸听等伪科学内容的；

（五）宣扬不良交友、恋爱观的；

（六）宣扬“读书无用论”“唯分数论”“唯升学论”等观念的；

（七）其他宣扬违反公序良俗和社会公德的不良价值导向的。

第五条　不当使用未成年人形象的信息包括但不限于：

（一）利用未成年人形象摆拍演绎含有不良价值观或者不当言行的剧情内容的；

（二）利用未成年人形象展示营销不适宜未成年人的产品与服务的；

（三）利用未成年人声线传播不良内容的；

（四）通过恶搞未成年人、利用未成年人打造争议人设等方式博取关注的；

（五）借未成年人在短视频中长时间摆拍积累人气、牟取利益的；

（六）以不良方式或者目的对未成年人进行品行、道德方面测试的；

（七）歪曲或者炒作涉未成年人违法犯罪行为的；

（八）其他不当披露和使用未成年人形象的。

第六条　不当披露和使用未成年人个人信息包括但不限于：

（一）未经监护人同意不当展示不满十四周岁的未成年人学习、生活等可能暴露未成年人个人信息的；

（二）诱导未成年人发布可能泄露本人或者他人个人信息的；

（三）其他不当披露和使用未成年人个人信息的。

第七条　对可能影响未成年人身心健康的网络信息，网络信息内容生产者以及网络产品和服务提供者应当按照《网络信息内容生态治理规定》、《网络暴力信息治理规定》等法律法规规定要求，采取防范和抵制措施，避免影响未成年人身心健康。

第八条　对于可能影响未成年人身心健康的网络信息，制作、复制、发布、传播该信息的组织和个人应当按照《未成年人网络保护条例》要求，在信息展示前，在明显位置作出显著提示。

网络产品和服务提供者应当为用户提供添加显著提示效果的标识功能，并引导和规范用户对相关信息作出提示。具体提示方式包括：

（一）在文本的起始、末尾或者中间适当位置添加文字提示或者通用符号提示等标识，或者在交互场景界面或者文字周边添加显著的提示标识；

（二）在音频的起始、末尾或者中间适当位置添加语音提示或者音频节奏提示等标识，或者在交互场景界面添加显著的提示标识；

（三）在图片的适当位置或者在交互场景界面添加显著的提示标识；

（四）在视频起始画面和视频播放周边的适当位置添加显著的提示标识，可在视频末尾和中间适当位置添加显著的提示标识，或者在交互场景界面添加显著的提示标识；

（五）呈现虚拟场景时，在起始画面的适当位置添加显著的提示标识，可在虚拟场景持续服务过程中的适当位置添加显著的提示标识；

（六）符合其他服务场景特点的显著提示标识方式。

第九条　网络产品和服务提供者应当落实《未成年人网络保护条例》要求，不得在首页首屏、弹窗、热搜、榜单、推荐、精选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，呈现可能影响未成年人身心健康的网络信息。

提供算法推荐、生成式人工智能等服务的，应当建立健全安全管理制度和技术措施，不得向未成年人推送可能影响其身心健康的网络信息。

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、传播可能影响未成年人身心健康的网络信息。

第十条　违反本办法规定的，依据《中华人民共和国网络安全法》、《未成年人网络保护条例》等法律、行政法规的规定予以处理。



关于印发《网络安全标识管理办法》的通知

各省、自治区、直辖市网信办、通信管理局、公安厅，新疆生产建设兵团网信办、公安局，中央和国家机关有关部门，各有关单位：

现将《网络安全标识管理办法》印发给你们，请遵照执行。

国家互联网信息办公室

工业和信息化部

公安部

2026年4月2日

网络安全标识管理办法

第一章 总则

第一条 为提升产品的网络安全能力，加强消费者权益保护，维护网络安全和公共利益，根据《中华人民共和国网络安全法》等法律法规，制定本办法。

第二条 本办法所称网络安全标识，是指能够反映产品本身网络安全能力水平的信息标识。

具有互联网联网功能的产品适用于本办法，具体产品实施目录管理。

第三条 网络安全标识管理工作坚持统筹发展和安全，产品生产者按照自愿原则参与。

鼓励产品生产者依据本办法提升产品网络安全能力，标注网络安全标识。

鼓励消费者优先选用标注网络安全标识的产品。

第四条 国家互联网信息办公室、工业和信息化部、公安部负责网络安全标识管理工作，分批制定公布《实施网络安全标识的产品目录》，明确每类产品的具体实施规则和依据的国家标准或技术文件，组织开展网络安全标识宣传教育，委托中国电子技术标准化研究院（以下简称备案机构）承担网络安全标识备案、信息发布等工作。

第二章 标识实施

第五条 网络安全标识对应的网络安全能力由低到高依次为基础级、增强级、领先级，相应的标识等级分别用一星、二星、三星表示。基础级要求产品应当满足相关国家标准的基本安全要求，如不存在弱口令或通用默认口令、建立漏洞管理机制并动态修复漏洞、保持软件更新等；增强级要求产品网络安全能力达到同类产品先进水平；领先级要求产品网络安全能力达到同类产品领先水平，同时还应通过渗透性测试方法，检测抵御高级别网络攻击的能力。

每类产品的标识等级具体安全要求，在实施规则中确定。安全要求应当和现行国家标准、国际标准做好衔接，充分借鉴吸收其它实施网络安全标识制度国家和地区的相关经验。

第六条 网络安全标识（英文名称为China Cybersecurity Label）应当包括以下基本内容：

（一）产品生产者名称；

（二）产品规格型号；

（三）网络安全能力等级；

（四）网络安全标识有效期；

（五）检测实验室名称；

（六）依据的国家标准或技术文件编号；

（七）备案信息码，通过扫码可以获取检测报告、关键指标、产品生产者符合性声明等信息。



每类产品标识的具体样式应当在对应的实施规则中明确，可根据产品实际形态在上述基本样式基础上适当调整。

第七条 需要标注网络安全标识的产品，产品生产者应当依据实施规则相关要求开展网络安全能力检测，确定网络安全能力等级，并取得检测报告。

（一）需要标注一星级、二星级的产品，产品生产者可以利用自有检测实验室或者委托依法取得资质认定的第三方检测机构开展检测；

（二）需要标注三星级的产品，产品生产者在满足有关检测要求基础上，还应当委托符合条件的第三方检测机构开展渗透性测试。

第八条 备案机构建设网络安全标识备案管理平台，产品生产者备案网络安全标识通过平台线上办理。

备案时应当提交以下材料的电子版：

（一）网络安全标识备案表；

（二）网络安全能力等级检测报告；

（三）依据实施规则设计的本产品网络安全标识样式；

（四）产品生产者符合性声明；

（五）产品生产者营业执照；

（六）自有检测实验室的相关检测能力证明材料，或者第三方检测机构相关资质认定证书；

（七）由代理人提交备案材料的，还应当提交产品生产者的委托代理文件等。

产品生产者及代理人应当对上述材料的真实性、准确性、完整性负责。

第九条 备案机构应当自收到完整备案材料之日起10个工作日内，对材料的真实性、准确性、完整性进行形式审查，完成备案工作并公告产品相关备案信息。

备案完成后，产品生产者可以按照实施规则要求印制、使用和展示网络安全标识。

第十条 网络安全标识有效期在相关产品实施规则中明确。备案完成的产品，关键技术参数等发生变更可能影响产品网络安全能力的，或者标识超过有效期的，应当重新备案。

第十一条 任何组织和个人不得伪造、冒用网络安全标识或者利用网络安全标识进行虚假宣传。

第十二条 备案机构应当建立健全网络安全标识备案工作规范，客观、公正开展网络安全标识备案相关工作。

产品生产者自有检测实验室或者第三方检测机构应当严格按照有关标准开展检测，保证检测结果客观公正、真实准确，不得伪造检测结果或者出具虚假检测报告。

备案机构和检测机构不得泄露在工作中知悉的国家秘密、商业秘密。

第三章 监督管理

第十三条 国家互联网信息办公室、工业和信息化部、公安部负责组织对网络安全标识备案、使用情况进行监督检查，发现有违反本办法规定行为的，按照有关规定及时处理。

地方网信部门、通信管理局、公安机关负责组织对本区域内网络安全标识使用进行监督检查，强化信息共享，发现有违反本办法规定行为的，应当会同相关部门按照有关规定处理，并及时通知备案机构。

第十四条 发现以下情况，备案机构应当撤销备案并及时公告：

（一）备案材料弄虚作假的；

（二）网络安全标识与实际网络安全能力不相符的；

（三）使用的网络安全标识不符合有关样式、规格等标注规定的；

（四）产品生产者终止对备案产品开展技术支持服务的；

（五）其他应当撤销备案的违规行为。

第十五条 产品生产者伪造、冒用网络安全标识或者利用网络安全标识进行虚假宣传的，备案机构应当撤销相关产品的网络安全标识备案，对产品生产者违规行为予以公告，自公告之日起一年内不再受理其产品备案。

第十六条 产品生产者自有检测实验室或者第三方检测机构伪造检测结果或者出具虚假检测报告的，备案机构应当撤销相关产品的网络安全标识备案，对检测机构违规行为予以公告，自公告之日起一年内不再采信其检测结果。

第十七条 产品生产者、第三方检测机构等发生网络安全能力检测弄虚作假、伪造冒用网络安全标识等行为的，由有关主管部门按照《中华人民共和国网络安全法》、《检验检测机构监督管理办法》等法律法规进行处罚。

第十八条 任何组织和个人发现违反本办法规定的行为，可以向地方网信部门、通信管理局、公安机关举报。地方网信部门、通信管理局、公安机关应当及时调查处理，并为举报人保密，调查过程中备案机构应当予以配合。

第十九条 网络安全能力检测过程中发现或者获知产品安全漏洞的，应当按照《网络产品安全漏洞管理规定》有关要求进行报告、修补和发布。

第二十条 国家互联网信息办公室、工业和信息化部、公安部等对违反本办法规定的行为建立信用记录，并纳入全国信用信息共享平台。

第四章 附则

第二十一条 本办法所称网络安全能力，是指产品生产者通过采取必要技术和管理措施，使产品本身具备防范攻击、侵入、干扰、破坏和非法使用，保障产品稳定可靠运行和网络数据完整性、保密性、可用性的能力。

第二十二条 网络关键设备和网络安全专用产品依据国家互联网信息办公室、工业和信息化部、公安部、财政部、国家认证认可监督管理委员会《关于调整网络安全专用产品安全管理有关事项的公告》（2023年第1号）开展安全管理，不列入《实施网络安全标识的产品目录》。

第二十三条 本办法自2026年7月1日起施行。

市人民政府关于印发武汉市支持人工智能OPC创新发展若干措施的通知

各区人民政府，市人民政府各部门：

经研究，现将《武汉市支持人工智能OPC创新发展若干措施》印发给你们，请认真贯彻落实。

武汉市人民政府

2026年2月13日

武汉市支持人工智能OPC创新发展若干措施

为抢抓人工智能发展机遇，培育本土科创新势力，激发全社会创新创业活力，推动科技创新和产业创新，加快打造国家科技创新中心，制定本措施。

一、强化算力服务支撑。加大普惠算力供给，建设涵盖算力统一流程、统一认证，算力供需对接、算力服务交易、算力储备的市级算力公共服务平台。设立算力服务券，对人工智能OPC（即由具备AI应用开发与整合能力的人才或者微型团队创办，以大模型为基础，AI编程、智能体等为核心工具，在研发、生产、运营等全流程实现效率超线性放大的“AI＋超级个体”新型创业实体，以下称OPC）当年支持周期内使用算力服务费用的50%给予最高20万元补助，补助期限不超过3年。（责任单位：市数据局、市经信局）各区在OPC生态社区集聚一批智能算力服务商，通过软硬件协同优化与高效调度技术，整合异构算力资源，提高算力利用效率，每年为每家OPC提供不少于2000卡时的免费算力支持。（责任单位：各区人民政府〈含开发区、长江新区、风景区管委会，下同〉）

二、畅通高质量数据要素供给。夯实公共数据底座，系统归集整合医疗、气象、时空、交通、政务等领域公共数据，落实

垂直领域模型，对于性能先进的模型，依规对研发单位按照国家首批数据流通利用试点任务，以“汉数通”平台为枢纽，构建“原始数据不出域，可用不可见”的数据应用环境，为OPC提供安全可信、合法合规的数据资源。加大行业数据应用力度，鼓励掌握行业语料资源的市场主体，围绕生产制造、能源优化、药物研发等领域提供高质量数据集，结合数据加工处理等技术，实现行业数据、语料产品开发定制。降低数据获取成本，支持OPC利用数据产品用于人工智能相关研发，对经认定符合要求的单位给予最高200万元补助。（责任单位：市数据局）开辟国际数据通道，为OPC生态社区开设国际互联网数据专用通道，支持OPC便利化获取全球数据资源。（责任单位：市委网信办）

三、支持模型工具研发应用。鼓励各类创新主体研发轻量化开发工具、低代码平台及垂直领域模型工具，攻关智能体高效开发框架；针对OPC在垂直行业落地中面临的技术瓶颈，支持OPC出题，高校院所、新型研发机构揭榜答题，实现技术供给与产业需求精准对接与协同研发，对经评定符合条件的项目，纳入市级重点研发计划，给予最高100万元资金支持。（责任单位：市科创局，各区人民政府）支持OPC打造垂直领域模型，对于性能先进的模型，依规对研发单位按照研发成本的30%给予最高500万元补助。支持OPC通过调用第三方大模型API（应用程序编程接口）或者采用本地化部署等方式，开展大模型垂直领域应用，依规按照不超过模型采购费用的50%给予最高100万元补助。（责任单位：市经信局）

四、构建人才“引育用留”体系。定期发布“招贤榜”，帮助OPC发布优薪优岗，组织开展人工智能领域引才活动不少于50场。（责任单位：市人社局）支持OPC引进具有知名人工智能企业2年以上研发经历的紧缺人才，支持OPC人才申报武汉英才计划，对入选战略科技人才、科技产业领军人才、优秀青年科技人才等专项的OPC人才，按照相关规定分别给予100万元、50万元、20万元资助。（责任单位：市人才工作局）市属高校联合人工智能企业、创新平台开展校企协同育人试点，共建OPC创业实践基地，将实践成果纳入学分认定体系；在汉部属、省属高校可参照执行。推动行业人才转型，面向金融、制造、医疗等领域的资深从业者，开展智能体应用专项培训，引导其面向行业需求创办OPC。（责任单位：市教育局、市人社局）加强OPC人才安居保障，构建“一张床、一间屋、一套房”政策性住房保障体系，让在汉创业的OPC人才“留得下、住得好”。提档升级“武汉青年人才之家”，为来汉创业就业的OPC人才提供最长15天免费住宿。对租住人才租赁房的OPC创业者，按照全日制博士研究生标准，给予2年且每月不超过2000元的免租优惠，第3年按照不高于市场上同类房产租金的70%缴纳租金。对OPC创始人及高管在我市购买新建商品房的，由商品房所在区按照每平方米1000元给予最高10万元购房补贴。（责任单位：市住房和城市更新局，市人才工作局，市财政局，团市委，各区人民政府）

五、大力发展OPC生态社区。各区结合“一城三廊多带”建设和城市更新规划，布局建设一批“低成本空间＋全链条生态服务”OPC生态社区，为入驻OPC提供普惠算力、数据资源、测试评估等专业服务，以及低成本办公空间、政策服务、场景对接、金融投资、商业配套等生态服务。东湖高新区建设OPC生态创新集聚区，依托现有产业园拓展布局一批OPC生态社区。中心城区通过盘活闲置楼宇，打造“生产、生活、生态”融合的OPC生态社区。鼓励在汉高校整合校内空间和要素资源，联合所在区共建OPC生态社区。制定OPC生态社区认定标准，定期开展认定、评估工作，依规给予OPC生态社区最高500万元资金支持。（责任单位：市科创局，各区人民政府）

六、提供创业启动支持。支持人工智能领域人才在汉创办OPC，综合评定其经营发展、技术创新情况，给予初创企业最高100万元的创业资助。（责任单位：市人才工作局）OPC生态社区构建与企业质量和发展阶段相匹配的支持政策体系，对入驻项目从技术创新性、成熟度、市场潜力等维度开展综合评定，梯度匹配涵盖租金减免、启动资金、“拨转股”、长期租金转股权等形式的支持政策。各区整合区内中试平台、概念验证中心及各类中介服务资源，为符合条件的OPC提供最长2年的免费公共服务包，涵盖财务代账、税务申报、法律咨询及专利申报等。（责任单位：各区人民政府）

七、搭建OPC线上开放社区。依托“武创通”科创服务平台打造OPC线上开放社区，吸引人工智能领域创业者、企业、高校院所和服务机构入驻，融合技术社群交流、开源项目协同、轻量化工具集成、人才培训与招募、政策精准推送、场景智能匹配等功能。设立专业技术交流与开源共享专区，支持技术分析、代码协作与难题解答，集成或者对接主流AI开发框架、开源模型及智能体开发工具。设立应用场景对接与方案推广专区，常态化征集发布真实业务需求、技术瓶颈、标杆案例。探索设立“AI产品体验券”，支持在汉大学生体验OPC线上开放社区发布的AI产品，培育潜在OPC创业者，加速AI产品推广应用。（责任单位：市科创局，武汉投控集团）

八、加大场景资源开放。加大场景开放力度，打造更多综合性重大场景、行业领域集成式场景、高价值小切口场景。支持行业主管部门、企事业单位向OPC开放政务服务、教育、医疗、公共安全等应用场景。定期在OPC线上开放社区发布“场景机会清单”“技术能力清单”，开展智能匹配与精准推送。（责任单位：市经信局、市发改委、市政府国资委，武汉投控集团）各区组建工作专班，中心城区围绕滨江数创大走廊建设和城市更新重点任务，开发区面向产业创新需求，新城区聚焦传统产业转型升级，为OPC挖掘、梳理和对接场景需求，全市每年挖掘不少于100个OPC典型应用场景。（责任单位：各区人民政府）举办“武创荟”科技成果转化OPC专场活动，精准开展人工智能创新成果路演、应用场景供需对接。（责任单位：市科创局，各区人民政府）每年遴选一批示范应用场景项目，按照项目总投入的30%给予最高100万元资金支持。（责任单位：市经信局）

九、强化科技金融支撑。构建“投保贷”联动的投融资服务体系，加大对OPC综合金融支持力度。发挥政府种子基金作用，建立OPC投资绿色通道，定期举办OPC专场投融资对接活动，用好“路演即投决”一体化机制，与市级人工智能产业基金形成接续式投资矩阵。（责任单位：市财政局，武汉投控集团、武汉金控集团）鼓励保险公司开发“种子项目投资保”等产品，对获得投资的OPC种子项目“见投即保”，降低企业早期研发活动风险。（责任单位：市科创局，市委金融办）

将符合条件的OPC纳入科技型企业知识价值信用贷款支持范围，联合银行推出“算力贷”，缓解企业在高性能算力服务采购中的资金压力，单笔贷款最高1000万元，对发生的贷款本金损失，给予最高80%的风险补偿。（责任单位：市科

创局，市委金融办，市财政局）为符合条件的OPC创业者提供最高30万元、最长3年的创业担保贷款，其中，对10万元以下的创业担保贷款免除反担保要求；为符合条件的OPC提供最高500万元、最长2年的创业担保贷款。（责任单位：市人社局、市财政局，团市委）

十、营造浓厚创新创业氛围。依托“武创荟”活动品牌，高水平举办OPC创新创业大赛，每年发掘不少于50个技术前沿、模式新颖、潜力巨大的标杆项目，并按照规定给予政策支持。建立大赛与市级人才计划直通机制，对符合条件的获奖团队核心成员，优先推荐申报武汉英才计划。（责任单位：市科创局，市人才工作局，武汉投控集团、武汉金控集团，各区人民政府）鼓励OPC生态社区、高校院所、投资机构、专业科技服务机构、OPC代表等共同发起成立OPC创新创业联盟，支持联盟成员单位常态化举办OPC主题展会、高端论坛、前沿技术研讨会、创投沙龙等活动；各区因地制宜，结合组织成效、品牌影响力等标准设置评价体系，按照规定给予活动主办方奖励支持。（责任单位：各区人民政府）

本措施自2026年3月18日起施行，有效期至2028年12月31日。

武汉市人工智能OPC生态社区建设指引

为推动武汉市人工智能OPC创新发展，构建全链条、便利化、低成本的创新创业服务生态，培育建设一批高质量人工工智能OPC生态社区，制定本指引。

本指引所称人工智能OPC（以下简称OPC），是指由具备AI应用开发与整合能力的人才或者微型团队创办，以大模型为基础，AI编程、智能体等为核心工具，在研发、生产、运营等全流程实现效率超线性放大的“AI＋超级个体”新型创业实体。本指引所称OPC生态社区，是指由各区主导建设，依托区域产业基础与创新资源，具备创业空间、算力调度、数据开放、模型工具、投融资对接、综合服务等功能，为OPC提供全链条、便利化、低成本服务的创新创业集聚区。

一、工作目标

营造有利于OPC创新发展的良好生态，统筹布局一批“低成本空间＋全链条生态服务”的OPC生态社区，构建集创业空间、算力调度、数据开放、模型工具、投融资对接、综合服务等功能为一体的“一站式”创新创业高地，推动形成以人工智能为支撑的OPC创新创业新范式。各区结合“一城三廊多带”建设和城市更新规划，科学布局OPC生态社区，聚焦智慧医疗、数字创意、城市服务、网络安全、工业软件、智能芯片、自动驾驶等一个或者多个优势领域，形成差异化、专业化发展格局。

到2026年底，建成3个OPC生态社区。到2028年，东湖高新区打造 OPC 创新集聚区，建成 3 个 OPC 生态社区；中心城区实现 OPC 生态社区全覆盖；全市 OPC 生态社区超过 10 个，其中具有示范效应的标杆型社区 2—3 个；集聚 OPC 人才 5000 人；孵化 OPC 企业 500 家。

二、建设主体

各区政府统筹推进OPC生态社区建设，加强资源要素供给和政策支持力度，引入或者培育具备产业生态构建能力的市场化专业机构作为社区运营方，开展社区品牌打造、生态构建、算力调度、数据开放、场景推进、招商协同与日常服务，运营团队应当具有丰富的人工智能行业经验、资源整合与孵化投资能力，主动链接产业资源、资本市场与应用场景。

三、基本条件

（一）专业服务：具备接入或者高效链接普惠算力、高质量数据集、主流开发工具与模型的能力，为入驻OPC提供算力补贴、数据资源、模型服务等支持。

（二）场地设施：核心办公面积不少于3000平方米，入孵人工智能相关企业不少于20家，其中OPC不少于10家。为入驻者提供租金减免、拎包入住、零租工位、设施共享等便利。

（三）金融服务：设立专项投资基金，建立快速投资决策机制，为OPC提供投融资支持。社区入驻金融机构不少于2家，每年组织投融资路演活动不少于5场。

（四）生活配套：周边或者内部应当具备人才公寓、餐饮、商务等生活与商业服务设施，满足OPC创业者便捷生活需求，构建10分钟办公生活圈。

（五）公共服务：整合区域内中试平台、概念验证中心及各类中介服务资源，为OPC生态社区入驻企业提供最长2年的免费公共服务包，涵盖财务代账、税务申报、法律咨询及专利申报等。

（六）生态活动：举办创新创业赛事、创新资源对接、创业培训等活动，为OPC提供多元化交流合作渠道。每年组织活动不少于10场。

（七）场景支持：所在区组建专班，每年为社区内OPC挖掘不少于20个应用场景，促成不少于5个场景落地。

四、认定流程：

市科创局每年发布OPC生态社区认定通知，明确申报时间、材料要求及流程。各区科创管理部门负责审核推荐。市科创局组织专家论证和现场核实，经集体研究、公示等程序，正式认定为OPC生态社区。

五、政策支持：

依据OPC生态社区认定标准与评估结果，对符合条件的OPC生态社区给予最高500万元资金支持。

喜报！武汉市网络安全协会党支部荣获“全市先进基层党组织”称号

赓续红色血脉，凝聚奋进力量。6月30日，武汉市“两优一先”表彰大会隆重召开，武汉市网络安全协会党支部被中共武汉市委授予“全市先进基层党组织”荣誉称号。这份沉甸甸的荣誉，是市委对协会党支部深耕两新党建、以党建引领网络安全产业发展的高度认可，更是对协会在市委网信办主管指导下，深度融入全市网信事业大局所取得显著成绩的充分肯定。

协会党支部自成立以来，始终坚持以习近平新时代中国特色社会主义思想为指引，深入学习贯彻习近平总书记关于网络强国的重要思想和总体国家安全观，旗帜鲜明把政治建设摆在首位。支部严格落实“三会一课”、组织生活会等组织生活制度，常态化开展联学共建、红色研学、专题党课，持续夯实基层战斗堡垒，切实将党的政治优势转化为推动行业发展的强大动能。



聚焦“党建红”引领“网安蓝”，协会党支部始终坚持以习近平新时代中国特色社会主义思想为指引，将党建与业务同频共振。在市委网信办及各级主管部门的悉心指导下，支部充分发挥战斗堡垒作用，以高质量党建引领行业高质量发展，在产业协同、标准建设、人才培育、社会服务等方面交出了亮眼答卷。

在**产业协同**上，支部以联建共建为纽带，牵头运营国家网安基地产业联盟，组建专家智库，搭建政企沟通与供需对接平台，积极开展招商引企，有效推动智能网联汽车、人工智能安全、医疗卫生健康等细分领域协同发展，为武汉网安产业集聚注入红色动能。

在**标准建设**上，支部紧跟行业前沿，主导研制并率先发布智能网联汽车网络安全检测、网络安全风险量化评估等团体标准，填补国内相关领域空白，并通过国标委备案，同时持续开展标准宣贯与前瞻立项，以标准化引领行业规范发展。

在**社会服务**上，支部坚持以人民为中心，深入开展网络安全“七进”活动，创新“文旅+科普”等宣传形式，聚焦老年人、青少年等群体开展“银发守护”“网安进校园”等行动，切实履行“网络安全为人民”的行业使命，让党旗在网安一线高高飘扬。

一名党员就是一面旗帜。在应急支撑、公益服务、政策辅导、产业赋能、人才培养一线，支部党员始终主动担当、冲锋在前，以实际行动践行初心使命，打造出党建引领网安产业发展的“武汉样板”。

“获评全市先进基层党组织，是激励更是责任。”协会党支部书记刘悦恒表示，这份荣誉是对过去工作的充分肯定，更是对未来发展的有力鞭策。下一步，协会党支部将以此次表彰为新起点，持续深化党建与产业融合，进一步发挥先进基层党组织示范带头作用，凝聚全市网络安全行业力量，全力服务国家网络安全人才与创新基地建设，以更高标准、更实举措推动武汉网络安全事业高质量发展，为筑牢新时代网络安全屏障贡献更大力量！



湖北党员生活杂志社、常青街道党工委莅临我会指导党建工作



为深入挖掘并总结基层党建创新实践经验，凝聚党建引领行业发展合力，近日，《党员生活》全媒体采访中心主任赵雯、江汉区常青街道党工委副书记饶玥率相关同志一行，莅临武汉市网络安全协会开展党建工作专题调研指导。

协会党支部书记刘悦恒热情接待调研组一行，全体支部委员参与。会上，协会党支部向调研组详细汇报了支部建设整体情况，重点围绕五大核心工作维度展开介绍：一是创新党组织共建机制，精准拓展行业党建覆盖广度，构建多方联动的党建工作格局；二是强化政治引领核心作用，持续筑牢党员干部思想根基与行业思想防线；三是深化党建与业务融合赋能，以党建“红色引擎”驱动业务发展，精准服务区域网络安全治理；四是主动践行社会责任，牵头夯实行业自律体系，引领行业规范发展；五是完善内部治理机制，着力锤炼政治过硬、业务精湛的党员队伍。

汇报中，协会党支部还具体阐述了在法规学习与标准研讨落地、网络安全专业人才培育、公益科普服务开展、支撑国家网络安全人才与创新基地建设等核心业务领域的党建融合实践成果，系统展现了协会打造具有网络安全行业鲜明特色党建品牌的探索与成效。

“获评全市先进基层党组织，是激励更是责任。”协会党支部书记刘悦恒表示，这份荣誉是对过去工作的充分肯定，更是对未来发展的有力鞭策。下一步，协会党支部将以此次表彰为新起点，持续深化党建与产业融合，进一步发挥先进基层党组织示范带头作用，凝聚全市网络安全行业力量，全力服务国家网络安全人才与创新基地建设，以更高标准、更实举措推动武汉网络安全事业高质量发展，为筑牢新时代网络安全屏障贡献更大力量！

武汉市网络安全协会党支部与市计量标准质量研究院第六支部开展联学共建主题党日活动

2026年1月28日下午，武汉市网络安全协会党支部与市计量标准质量研究院第六支部在国家网络安全人才与创新基地联合开展“党建引领聚合力，联学共建促发展”主题党日活动。协会党支部书记刘悦恒主持活动，双方全体党员参加。

活动组织参观了国家网络安全人才与创新基地展厅，重温了入党誓词，集中学习了党的二十届四中全会精神及省、市相关工作会议精神。市计量标准质量研究院第六支部黄勇同志作了《以标准引领促网络安全健康发展》专题党课的学习。党员代表结合“十五五”规划落实进行了交流发言。

双方支部书记在总结中一致认为，此次活动促进了理论共学、业务共融、支部共进。未来双方应建立常态化交流机制，在标准制定、安全评估等领域开展项目化协作，共享资源、优势互补，共同为武汉网络安全产业高质量发展贡献力量。







市公安局网安支队六大队与市网络安全协会联合开展“迎七一·强党性·保安全”主题党日活动

赓续红色血脉 警会协同护网

回望来时路 红色教育淬炼党性

2026年6月30日下午，在中国共产党成立105周年即将到来之际，武汉市公安局网络安全保卫支队六大队党支部与武汉市网络安全协会党支部在武汉警察博物馆联合开展“迎七一·强党性·保安全”主题党日活动。双方党员通过共学党史、共研安全、共谋发展，深化了警会协同共识，凝聚了守护网络空间的强大合力。

活动在承载着厚重公安历史的武汉警察博物馆举行。这座华中地区首座以警察历史文化为主题的博物馆，通过4000余件实物藏品、历史档案与场景复原，全景展现了武汉公安从近代至今维护稳定、服务人民的忠诚足迹。在讲解员的带领下，全体党员集体参观了禁毒英烈展区，党员们驻足学习全国公安英模烈士的感人事迹，并参观了正在展出的“英雄之城 无毒之路”禁毒主题展览。全体党员在泛黄的历史照片、珍贵的实物展品前驻足凝视，深入了解武汉公安在不同历史时期的奋斗历程。参观结束后，全体党员面向党旗庄严宣誓，铿锵誓言回荡在博物馆大厅，彰显了“公（网）安蓝”与“党旗红”深度融合、共筑网络安全屏障的坚定信念。

走好当下路 联学共建护航发展

在书记领学环节，武汉市公安局网安支队六大队党支部副书记、教导员罗利文抛开大道理，跟大家聊起了“怎么才算干得好”。他说，网安工作不能光盯着打击破案，老百姓觉得上网安全、踏实，才是硬指标。“有些活儿虽然藏在屏幕后面没人看见，但咱们得甘当‘隐形卫士’，把基层的地基打牢。”他号召大家既要能干大事，也要耐得住寂寞，实实在在地守好网络安全的大门。

随后，武汉市网络安全协会党支部书记、秘书长刘悦恒带领大家聚焦习近平总书记在二十届中央政治局第二十四次集体学习时的重要讲话《前瞻布局和发展未来产业》。学习内容中强调，面对量子科技、脑机接口、具身智能等前沿领域带来的安全挑战，必须将网络安全作为新质生产力发展的根基。结合武汉建设全国科创中心的目标，双方党员聊得特别实在：不能等新产业长大了再补“安全课”，得提前帮企业“法治体检”，手把手解决数据安全的麻烦；还要多培养既懂技术又懂实战的“跨界”人才，让科技创新在安全的轨道上跑得更稳更快。

展望未来路 协同共治开创新局

座谈交流中，党员代表围绕“党建引领下的警会协同”踊跃发言。大家一致表示，此次活动通过“历史现场悟初心，前沿领域话使命”，深化了双方对“警会协同共治”的认识。未来双方将以党建为纽带，在风险预警、应急联动、技术攻关等方面拓展合作维度，构建“资源共享、优势互补”的协同机制，携手为武汉数字经济高质量发展筑牢安全底座，以实干实绩向党的105周年献礼。

武汉市网络安全协会党支部组织集中收看中国共产党成立105周年大会

历史川流不息，精神代代相传。7月1日上午10时，庆祝中国共产党成立105周年大会在北京人民大会堂隆重举行。武汉市网络安全协会党支部组织全体党员及工作人员集中收看大会直播，认真学习领会习近平总书记重要讲话精神。

大会庄重肃穆、气氛隆重热烈。习近平总书记的重要讲话高屋建瓴、思想深邃、内涵丰富。总书记重要讲话回顾了党的百年奋斗历程，深刻揭示了党始终不渝的为民初心和与时俱进的政治品格，强调要坚定信心、接续奋斗，不断创造无愧于时代和人民的新业绩。观看期间，全员凝神观看、认真记录要点，在总书记讲话中感悟初心使命，进一步筑牢理想信念之基。

不忘初心跟党走，砥砺奋进新征程。协会党支部将持续丰富党建学习载体，引导全体党员扛起网络安全社会责任，坚守数字安全阵地，以实干担当书写护航城市网络空间安全的崭新答卷！







武汉新增全国唯一网安类本科高校，今秋招生

网络空间，是继陆、海、空、天之后人类活动的“第五空间”，守护这片疆土，就是守护国家主权、人民福祉与数字经济未来。近日，教育部正式批复同意设置网络空间安全学院，这是全国唯一独立设置的网络安全类本科高校，计划于2026年秋季启动首批招生，首批设置人工智能、数据科学与大数据技术、软件工程、计算机科学与技术4个普通本科专业，精准对接国家战略与产业需求，为广大有志青年投身国家网络安全事业搭建起全新平台。



网络空间安全学院网安基地校区

权威官宣：全国唯一，武汉再添网安人才培养“新阵地”

日前，教育部已正式向湖北省发函，批复同意设置网络空间安全学院。作为公办普通本科高校，该学院无地域前缀的命名方式，凸显其服务国家整体安全格局的核心定位，将面向党政机关、关键信息基础设施运营机构、中央企业等，重点培养网络安全战略型、尖端型、实用型人才。



网络空间安全学院综合学习中心效果图

学院选址于武汉临空港经济技术开发区国家网络安全人才与创新基地，这里已形成浓厚的产业与人才集聚效应——不仅有武汉大学、华中科技大学两所“双一流”高校的网络空间安全学院，还汇聚了华为、天融信等400余家网络安全产业链上下游企业，构建起国内领先的网络安全产业、科技、教育融合发展生态圈，为学生提供了得天独厚的学习、实践环境。

作为学院办学根基，湖北武汉拥有得天独厚的科教优势，是我国中部地区科教资源最集中的城市之一，高校数量、科研院所规模均位居全国前列，尤其在网络安全领域，形成了从基础研究到人才培养、产业应用的完整生态。武汉集聚了武汉大学、华中科技大学等一批顶尖高校，其中两所高校的网络安全学院均入选全国一流网络安全学院建设示范项目。

而学院所在的国家网络安全人才与创新基地，是我国网络全领域的重点布局项目，也是国内首个“网络安全学院＋创新产业谷”模式的特色基地，总体规划面积40平方公里，核心区4平方公里已基本建成。目前，基地内注册企业超300家，汇聚了奇安信、天融信等网安头部企业。同时，基地拥有金银湖实验室、黄鹤实验室等一批网安领域新型研发机构，聚焦智能化软件安全、密码理论与应用等重点方向开展有组织科研，持续突破产业关键技术瓶颈，构建起“人才链、创新链、产业链”三链共振的发展格局。

此外，该基地还是全国唯一的国家关基行业安全保护培训基地，累计开展各类专业培训。基地还定期举办武汉网络安全创新论坛、中国研究生网络安全创新大赛等各类高水平活动，吸引全国顶尖专家学者、行业领袖齐聚，为学生搭建起交流学习、开阔视野的高端平台，真正实现“以产聚才、以才促创、以创兴产”的良性循环。

深度解读：国家布局，网安学科已成战略刚需

很多考生及家长可能会问，网络空间安全专业到底是什么？国家为何如此重视这一学科的建设？事实上，网络空间的竞争，归根结底是人才的竞争，而学科建设正是人才培养的根基。

从国家战略布局来看，网安学科的发展早已上升为国家意志：

2015年6月，国务院学位委员会、教育部正式在“工学”门类下增设“网络空间安全”一级学科，学科代码为“0839”，授予“工学”学位，标志着我国网安学科建设进入规范化发展阶段；

2016年12月，《国家网络空间安全战略》正式发布，明确提出实施网络安全人才工程，加强网络安全学科专业建设，打造一流网络安全学院和创新园区；

2017年6月，《中华人民共和国网络安全法》正式实施，明确国家支持高校、职业学校开展网络安全相关教育与培训，多方式培养网络安全人才；

截至目前，我国已建立起本科、硕士和博士等不同层次的网安人才教育培养体系，本科阶段开设网络空间安全专业的高校已达121所，同时确定11所高校为一流网络安全学院建设示范项目高校，其中武汉大学、华中科技大学均位列其中。

值得关注的是，当前我国网络安全人才供需失衡问题突出，根据教育部相关权威部门数据，预估目前专业人才累计缺口在140万以上，而每年相关专业高校毕业生规模仅2万余人，到2027年，人才缺口将达327万，92%的企业表示缺乏网络安全实战人才。选择网安专业，不仅是选择了一个前景广阔的赛道，更是选择了一份守护国家网络安全的责任与使命。

据了解，作为全国唯一独立设置的网安类本科高校，该学院在人才培养上极具特色，精准对接国家需求与行业痛点，为考生提供高质量的培养路径：

办学理念鲜明，育人机制创新——以“政治引领、能力导向、产教融合、兴趣教学”为办学理念，构建校企双导师制、双学分制和书院制“三制协同”育人新机制，探索“实网攻防、实岗训练、实操演练、实战检验”的育人新路径，着力培养“既能解决复杂问题、又能胜任复杂实战”的网络安全专业人才。

专业设置精准，课程紧贴实战——首批将设置人工智能、数据科学与大数据技术、软件工程、计算机科学与技术4个普通本科专业，精准对接国家网络安全战略与前沿产业需求。187门核心课程大纲将由在校教师与企业专家联合编纂，把企业最新的攻防案例、技术成果、岗位需求转化为教学项目，让课堂与行业前沿同频。

实践平台优质，产教深度融合——学院将与行业龙头企业深度合作，共建13个专业实验室和28个实习实训基地，把课堂变身“网络靶场”、作业成为“安全评估报告”、考试化作“真实电子对抗”，让学生从入校起就沉浸在真实的网络安全实战环境中，提升实操能力。

校企共建实验室

合作企业	挂牌名称
曙光信息产业股份有限公司	处理器安全及应用联合实验室
中金数据集团有限公司	算力中心
北京天融信网络安全技术有限公司	网络空间安全防护与运营实验室
北京数字认证股份有限公司	密码工程实验室
恒安嘉新（北京）科技股份公司	网络行为研究实验室
华为技术有限公司、武汉数据集团有限公司	网络传播与舆情安全实验室
浪潮工业互联网股份有限公司	工业互联网安全实验室
三六零安全科技股份有限公司	人工智能安全实验室
奇安信科技集团股份有限公司	网络安全产业联合实验室
武汉安域信息安全技术有限公司	网络安全攻防实验室
中汽智能科技（天津）有限公司	智能网联汽车信息安全实验室
武汉赛宝工业技术研究院有限公司	工业控制系统安全检测实验室
中国电信股份有限公司湖北分公司/天翼安全科技有限公司	智能云网安全实验室

网络空间安全学院部分校企共建实验室

武汉市网络安全协会呼吁：以青春之名，赴网安之约

作为武汉网络安全领域的行业纽带，武汉市网络安全协会始终致力于推动网络安全产业发展与人才培养工作。当前，数字经济蓬勃发展，网络安全已成为数字经济发展的基石，关乎国家利益、人民福祉，守护网络空间安全，需要一代又一代青年的接力奋斗。

武汉新增的网络空间安全学院，既是国家网络安全人才培养战略的重要延伸，也是武汉打造“网安高地”的重要举措，更为广大考生提供了一个投身国家网络安全事业的绝佳平台。在这里，你将系统学习网安知识、锤炼实战本领，成长为守护国家网络疆土的“尖兵”；在这里，你将与行业专家并肩、与优秀同伴同行，在网安领域实现个人价值与国家需求的同频共振。

青春逢盛世，奋斗正当时！武汉市网络安全协会郑重呼吁广大有志考生，抓住机遇、积极报考，选择网络空间安全专业和相关院校，选择守护国家网络安全的使命，以青春之力筑牢网络安全防线，用专业所长护航数字中国建设，在网络空间的“战场”上，书写属于新时代青年的责任与担当！

后续，武汉市网络安全协会将持续关注该学院招生动态，及时为广大考生提供相关资讯，助力大家顺利报考、圆梦网安！

综合信息来源：长江日报



全国唯一！首次开放

6月13日，全国唯一独立建制的网络安全类公办本科高校——网络空间安全学院，首届校园开放日活动在武汉市东西湖区（中国网谷）国家网安基地举办。

市委常委、宣传部部长吴朝安，东西湖区委书记王敏，市政府副秘书长、网络空间安全学院筹建负责人张明武等领导和嘉宾参加活动。

本次开放日设置网安领航见面会、趣味解码主题分享会、校园游园会三大板块，从政策交流、专业解读、实景体验多个维度，全方位展示了这所深度融入国家网安基地的高校办学特色、人才培养模式、专业实力与招生政策。

作为面向国家网络安全战略需求建设的新型高校，学校坚持“基地即大学，大学即基地；企业即大学，大学即企业”的创新办学模式。活动现场，华中科技大学网络空间安全学院院长分享校地合作与学科建设成果，奇安信、中科曙光、天融信、恒安嘉新、中金数据等一众入驻国家网安基地的头部企业高管现场发出报考倡议，并共同启动校企合作企业班，贯通人才培养、实训、就业全链条。

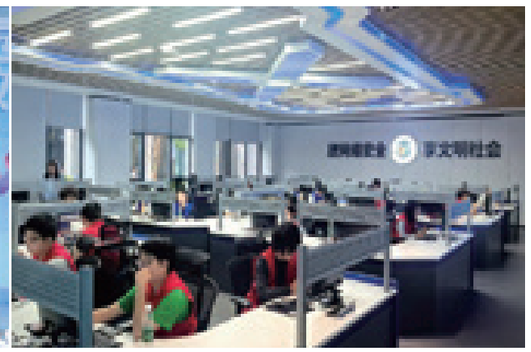
趣味解码主题分享会聚焦人才培养与招生政策。校方详细介绍校企双导师制与“实网攻防、实岗训练、实操演练、实战检验”四实育人路径。凭借多学科交叉的办学优势，构建起通识教育+专业教育+个性化教育的人才培养体系。招生有关负责人解读本年度湖北招生政策、参考分数线及志愿填报要点。三大专业学院结合真实岗位场景，讲解各专业课程设置、培养定位与职业发展方向，让参会人员清晰了解各专业特色与就业前景。

校园游园会作为核心体验环节，活动设置九大主题打卡点位，串联校园实训平台、科研载体、教学场馆、生活配套等全域场景。参访考生及家长沿专属导览路线沉浸式巡览校园全貌，近距离感受现代化、智慧化、实战化的办学环境。现场还布设20余家网安企业展区与学院专业展区，集中展示行业前沿技术与校企合作成果。

网络空间安全学院首次校园开放日效果火爆，数千名学生和家长参加本次校园开放日，在线直播观看人数超50万人次。

综合信息来源：东西湖区融媒体中心





2026年“黄鹤杯”网络安全人才创新大赛启幕

5月29日，2026年“黄鹤杯”网络安全人才创新大赛在武汉国家网络安全人才与创新基地正式启动。全国相关高校院所和领军企业的学者、专家、负责人与参赛代表共同见证赛事启幕。





大赛以“人机共战砺网安精兵　产才融合筑产业高地”为主题，在赛制与理念上创新引入独立AI攻防战队与人类选手同台竞技，从初赛到决赛全程融入模型逆向、提示词注入等AI安全专项考点，决赛采用“AWDPlus攻防对抗＋RW实物漏洞挖掘”双轨赛制，搭建智能网联汽车、低空飞行器、IoT物联网等实物靶场，重新定义AI时代网安竞技标准，彻底告别脱离业务的理论化演练，让比赛成果直接转化为实际战斗力。

大赛设学生组与职业组双赛道，7月上旬将举行覆盖十大网安领域的线上CTF夺旗赛，10月晋级队伍将齐聚武汉国家网安基地，与AI战队展开为期两天的线下巅峰对决。

大赛坚持“以赛促学、以赛选才、以赛兴业”，设置了丰厚的赛事奖项与全方位人才激励政策，各组获奖选手最高可获优秀企业直通面试实习机会，优先纳入网安人才库，优秀技术成果将获得产业孵化支持，对接落地应用。

为保障赛事专业权威与公平公正，大赛组建了覆盖高校科研、金融安全、工业互联网等全领域的全国顶尖专家团队，全程参与赛题研发、现场评审与争议裁定工作。同时构建三位一体全流程防作弊体系，切实保障每一位选手的权益。

目前，2026年“黄鹤杯”网络安全人才创新大赛全国报名通道已全面开启，报名截止时间为2026年6月30日。全国各高校、企事业单位均可登录大赛官方网站（https://hhb.whcsa.org.cn）报名，也可关注“武汉网络安全”官方微信公众号了解最新动态。

作为伴随国家网安基地建设应运而生，共同成长的专业赛事，“黄鹤杯”自2018年创办以来，累计吸引全国近万名选手参赛，推动百余项技术成果落地转化，为国家网信事业输送了大批实战型、应用型人才。组委会诚邀全国各单位积极组队参赛，与全国网安精英同台竞技、切磋交流，共同为国家网信事业发展和更高水平“中国网谷”建设贡献力量。

“中国网谷”科创政策矩阵发布 大型人工智能企业设总部最高支持2亿元

2月26日上午，东西湖区科技创新大会暨“中国网谷”建设动员大会举行。会上发布全域科创政策矩阵，链主企业建设研发中心最高可获1亿元支持，大型人工智能企业设立总部最高可获2亿元支持。

今年是“十五五”开局之年，也是“中国网谷”建设的关键之年。为此，东西湖区重点打造以网安基地为核心、多点布局的“一基地五圈层”科技创新空间布局，即国家网络安全人才与创新基地、环协和未来智慧医院科创圈层、数字创意科创圈层、总部经济科创圈层、数实融合科创圈层。

其中，国家网络安全人才与创新基地，作为全区科技创新的核心引擎，聚焦网络安全、信息安全、数据安全、人工智能安全、卫星互联网安全“五安”，以及数据服务、信创、智慧视觉、具身智能、智能终端领域“五域”，聚集科研院所优质打造网信数智领域创新型企业集聚发展首选地。



为加快推动创新链与产业链深度融合，东西湖区已构建以综合性科创政策为统领，面向人工智能、电子信息、氢能等11大产业专项政策为支撑，以“启元空间”管理办法和天使投资基金管理办法为配套的“1+11+2”政策矩阵，对科创主体的支持从“点状输血”迈向“制度性造血”。

“投资建设研发中心的链主企业，最高支持1亿元。建设全国或区域总部的人工智能大型企业，最高支持2亿元。”东西湖区相关负责人介绍，出台全域科创政策矩阵，旨在吸引科技总部落户，鼓励企业加速技术突破，加快科研成果转化，激励链主企业形成产业集群。

长江日报记者了解到，该区发布的全域科创政策矩阵还包括：对认定为国家级创新平台的牵头单位，给予500万元奖励。对购买高校院所科技成果的企业，最高补助100万元。对促成转化的技术转移机构，最高奖励150万元。

东西湖区主要负责人表示，开局之年当有开局之势，关键之年当有关键之为。要坚定不移抓牢高质量发展首要任务，以国家网安基地和陆港型国家物流枢纽为牵引，强化创新驱动、产业升级、环境营造，一步步把“中国网谷”发展蓝图变为美好现实。

数据显示，“十四五”期间，东西湖区高新技术产业增加值年均增幅达到13.6%，市级以上企业创新平台翻番增长至185家，市级以上众创孵化载体翻两番增长至18家，高新技术企业数量超1700家，技术合同成交额超140亿元，均是“十三五”末的5倍多。

综合信息来源：长江日报

武汉大学召开2026年度网络安全工作会议

4月27日，武汉大学召开2026年度网络安全工作会议，深入学习贯彻习近平总书记关于网络强国的重要思想，全面落实党中央、教育部、湖北省委关于网络安全工作部署，系统总结工作成效，分析当前形势，部署学校网络安全重点工作。校长张平文、副校长朱德友出席会议。

会议邀请有关专家以《提高网络安全意识，筑牢网络安全屏障》为主题开展宣讲，结合真实案例深入分析了当前网络安全面临的形势与挑战。信息中心负责人汇报了学校网络安全工作有关情况，总结存在的突出问题，明确下一步工作重点。

张平文强调，各单位要深刻认识网络安全工作的重要性，切实将党对网信工作的全面领导落到实处。他强调，要严格落实网络安全责任制，强化闭环管理，以练促防，扎实做好教育部网络安全攻防演练准备工作；要强化系统思维，把网络安全、数据安全纳入学校事业发展规划，优化“建网”“管网”“用网”工作机制，构建全方位、全要素、全周期的技术防护体系；要注重提升师生网络安全意识，持续深化宣传教育，加强国家网络安全学院建设，着力培养实战型、复合型、高水平网络安全人才。

各学院、职能部门、直属单位、研究机构及服务与经营性单位主要负责人、网络安全联络人参加会议。

综合信息来源：武汉大学信息中心



当“小龙虾”游入“中国网谷”：折射网安信创产业新生态

4月22日，香港资讯网安考察团到访位于国家网络安全人才与创新基地的天融信武汉研发中心，就AI安全、信创安全等主题座谈交流。此前，天融信集团成为国内网安厂商中唯一通过中国信通院OpenClaw类智能体安防产品能力评估的企业。

今年初，AI智能体OpenClaw（被开发者称为“小龙虾”）开源并迅速走红，其潜在的安全风险随之浮现。在武汉东西湖，这场由“小龙虾”引发的安全攻防，成为一个生动的观察切口，展现了“中国网谷”如何从应对具体威胁出发，构筑并打开一个更为坚实的网安信息技术应用创新产业生态。



天融信武汉研发中心

应战：在新型威胁前快速布防

在武汉，华科大武汉校友会路演厅里挤满前来“吃虾”的人；在深圳，腾讯大厦门口，近千名开发者与AI爱好者排队等待云端安装。

OpenClaw在展现强大能力的同时，其安全风险也受到监管关注。工信部及国家互联网应急中心相继发布了相关提示。

面对新型威胁，网安企业迅速回应。3月9日，恒安嘉新在其位于国家网络安全人才与创新基地的武汉研发中心，发布了OpenClaw安全治理产品（AIGov）。一周后，奇安信发布了国内首份《OpenClaw生态威胁分析报告》及《政企版龙虾（OpenClaw）安全使用指南》。



这种快速反应能力，源于长期的前沿技术投入。

早在去年4月，天融信科技集团就发布了智算一体机，旨在帮助企业降低AI应用门槛。更早的2023年，其自研的“天问”大模型已能实现未知威胁感知。设在基地内的这些研发中心，正是将深厚技术储备转化为实战能力的关键支撑。

网安攻防战场，“大厂”大招频出背后，是其设在国家网安基地研发中心、应急枢纽的强力支撑。

网安“国家队”从幕后走进高光时刻，东西湖区网安信创新兴产业历经萌芽与成长，迎来果实累累的收获期。

深植：近十年的基石与积淀

产业的快速反应，建立在深厚的根基之上。2016年，全国首个国家网络安全人才与创新基地落户东西湖区。

天融信科技集团是最早签约入驻的企业之一，累计投入16亿元，在此建成了其北京总部以外规模最大的综合性研发中心，现有研发保障人员超过500人。聚焦智能网联汽车发展，其30余项车联网安防产品已应用于比亚迪等头部整车厂。

产业联动在此不断深化。天融信武汉研发中心联合东风岚图成立了智能网联汽车网安专委会。以基地为纽带，武汉的“星谷”“光谷”和“网谷”共同组建了“武汉市卫星与应用产业创新联盟”。

此次香港考察团到访，开启鄂港网络安全合作新典范。国家网安基地AI安全、信创安全、数据安全等领域核心成果，将走进创新澎湃的大湾区。

经过近十年发展，国家网络安全人才与创新基地核心区已基本建成，注册企业超过400家，累计培育高新技术企业54家、规上企业36家，获评工信部“中小企业特色产业集群”。

恒安嘉新武汉研发中心助力集团深耕“云网边端业数智安”领域，反诈业务覆盖全国31省200余个地市。

奇安信集团落地近十年，累计投资超10亿元，其核心产品“天眼”威胁监测及分析系统连续四年位居国内市场第一。该集团计划再投资10亿元提升华中总部能级，并将“补天杯”破解大赛引入武汉。

成链：从安全底座到信创生态

以国家网络安全人才与创新基地为战略支撑，东西湖区着力构建“网信芯智端”核心产业，形成“网信创芯，智联万端”的发展格局。在筑牢网络安全底座的同时，产业生态正向信创领域加速拓展。

2023年6月，宝龙达集团在东西湖设立全球总部、全球研发中心和全国制造基地。2025年，集团产值突破90亿元，占据国内信创PC市场约八成的份额。在其智能产线上，平均每分钟有4台电脑下线。

宝龙达的到来，有力带动了产业链的集聚。为提升与上下游核心供应链企业的协同效率，集团正加紧实施供应链本地化战略，旨在中部地区形成完备的产业链体系和现代信息技术应用创新产业集聚区。

目前，宝龙达集团联手因大联科产业集团合力打造的第四代产业园“因大联科宝创·临空创智中心”正快速推进，持续完善信创与智能终端产业生态。

“从应对一个具体的AI威胁，到历经近十年构筑的国家级基地基石，再到牵引一条完整的信息技术应用创新产业链，东西湖‘中国网谷’的实践，展示了一个新兴产业从被动防护到主动布局、从单点防御到生态构建的升级之路。”武汉临空港网信自主创新产业商会会长田霞评价，这种基于深厚积淀、兼具快速响应与长远布局的能力，正是其打造产业高地的关键。

“提升网安信息技术应用创新产业发展能级，打造全国信创电脑产业高地。”根据规划，迈入“十五五”，东西湖区将依托龙头企业，建成具有全国影响力的网安信息技术应用创新产业集群。到2030年，该产业营业收入目标为500亿元。

从应对“小龙虾”威胁的快速“应战”，到国家基地近十年的深厚“深植”，再到信息技术应用创新产业链的集聚“成链”，一条清晰的产业演进路径已然呈现。

综合信息来源：东西湖区融媒体中心

武汉市网络安全协会第二届理事会第七次会议顺利召开

2025年12月27日，武汉市网络安全协会第二届理事会第七次会议在武汉市江夏区隆重召开。协会会长、副会长、理事出席会议，各分支机构负责人、部分会员代表及秘书处全体员工等共五十余人列席参加，共商协会发展大计，共谋武汉网络安全产业高质量发展新篇章，会议由秘书长刘悦恒主持。



本次会议紧扣行业发展脉搏，聚焦协会核心工作，共设置8项议程，内容涵盖工作总结、计划部署、规范修订、标准建设、会员发展等多个关键领域，旨在通过系统梳理过往成效、科学谋划未来方向，进一步凝聚行业合力，推动协会规范化、专业化发展。

会议强调，2025年作为“十四五”规划收官与“十五五”规划谋篇布局的关键之年，协会始终秉持“服务会员、服务行业、服务政府、服务社会” 的核心宗旨，以党建引领为根本，以规范建设为保障，以产业赋能为核心，在主管部门指导和全体会员支持下，各项工作取得显著成效。

会议要求，党建引领是协会发展的根本遵循，需持续深化理论学习、规范支部建设、践行社会责任，为行业发展提供坚强政治保障。



会议审议并通过了《协会2025年度工作总结（审议稿）》，通过了《协会2026年工作要点》。2026年协会将重点围绕强化党建引领、深化产业联盟运营、扩大会员覆盖与优化服务、推进标准体系建设、规范分支机构发展、强化宣传赋能、搭建产学研用协同平台、优化人才培养体系、深化公益服务与行业治理、完善内部治理与外部协作等十大方向开展工作，全力支撑国家网安基地建设，为武汉网络安全事业发展注入更强动力。

会议还逐一审议并通过了协会各分支机构2025年度工作总结，充分肯定了各分支机构在专业领域的积极作为与突出成效。智能汽车网络安全专委会、民办高校工作委员会、网络安全保险工作委员会、医疗卫生与健康分会、人工智能专业委员会等分支机构立足自身职能，在标准落地、供需对接、技术创新、人才培育等方面扎实推进工作，有效助力了重点领域网络安全能力提升。

为进一步规范内部管理、提升服务效能，会议审议通过了《关于对武汉市网络安全协会秘书处专职人员人事考核管理办法的修订建议》、《武汉市网络安全协会团体标准经费管理办法细则（草案）》、《武汉市网络安全协会新进会员流程规范（草案）》三项重要规范文件。这些文件的出台，将为协会人事管理、经费使用、会员发展等工作提供更科学、更具可操作性的制度保障，推动协会运营管理再上新台阶。

在标准化建设与行业规范方面，会议审议通过了《关于公开征集＜网络安全企业认定规范＞、＜网络安全产品和服务认定规范＞团体标准参编单位的提案》。两项团体标准的制定，将进一步规范武汉网络安全行业秩序，明确企业产品研发与安全服务的基线，为行业合规发展提供重要依据。协会将承担该标准编制费用，公开征集参编单位及人员，凝聚行业智慧共同推动标准落地。

会议一致同意，中国移动通信集团湖北有限公司武汉分公司、湖北大学网络空间安全学院成为协会第二届新晋理事单位；数字认证（武汉）有限责任公司、武汉东湖新技术开发区网盾职业培训学校有限公司等10家单位及1位个人获批入会。新成员的加入，为协会注入了新鲜血液，将进一步壮大协会力量，拓展行业服务覆盖面。

会议号召，全体理事与会员单位要以此次会议为契机，坚守初心、履职尽责，充分发挥行业引领作用，聚焦网络安全核心领域，深化协同合作、强化创新驱动、补齐发展短板，共同推动武汉市网络安全行业持续健康发展，为武汉在支点建设中当好龙头、走在前列提供坚实的网络安全保障。



武汉市网络安全协会2025年终团建交流活动圆满举办

为进一步增进各会员单位沟通情谊，凝聚网络安全行业协同发展合力，12月27日，武汉市网络安全协会组织开展-2025年终团建交流活动。协会理事单位、监事单位、各分支机构负责人及会员代表欢聚一堂，大家在轻松融洽的氛围里畅叙情谊、共谋发展，为2025年度各项工作画上圆满句号。

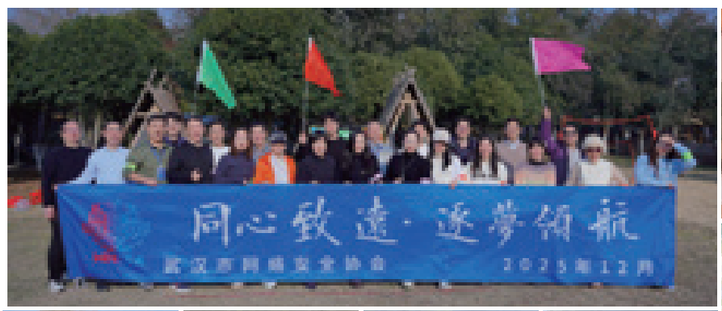
本次团建活动以“趣味互动、协作共赢”为核心，精心设计了多元化体验环节，兼顾休闲放松与团队协作，让参与者在活动中增进了解、凝聚共识。

极限飞盘主题团建成为活动亮点。在专业教练的指导下，参与者们分为多个战队，迅速投入到紧张有趣的竞技中。赛场上，大家秉持“盘不落地、永不放弃”的拼搏精神，默契配合、灵活跑位、精准传接，每一次精彩攻防都引来阵阵喝彩。这场充满活力的团队竞技，不仅考验了大家的反应能力与协作意识，更让彼此在并肩作战中加深了信任、凝聚了合力。

自由活动环节，丰富多样的体验项目满足了不同需求。

户外场地内，ATV越野车的轰鸣声此起彼伏，参与者们驾驭车辆驰骋赛道，感受速度与激情；在真人CS战场上，大家分组对抗、巧妙布局，在模拟实战中体验协作制胜的乐趣；采摘园内，新鲜的果蔬挂满枝头，大家结伴采摘，享受亲近自然的惬意。协会女性会员齐聚手工馆，在老师的带领下手工制作葫芦脐灸丸、手工香薰，让大家专注投入创作，在动手实践中放松身心、陶冶情操、增进情谊。

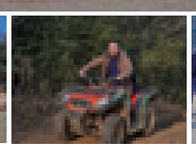
此次团建交流活动的成功举办，不仅为协会会员单位搭建了轻松交流的平台，更有效增进了行业内的凝聚力与向心力。大家纷纷表示，活动既缓解了日常工作的压力，又收获了珍贵的友谊与合作共识。未来，武汉市网络安全协会将继续秉持“服务会员、凝聚合力”的理念，持续搭建多元化交流平台，推动会员单位之间深化合作、携手共进，共同为武汉网络安全产业高质量发展注入更强动力。













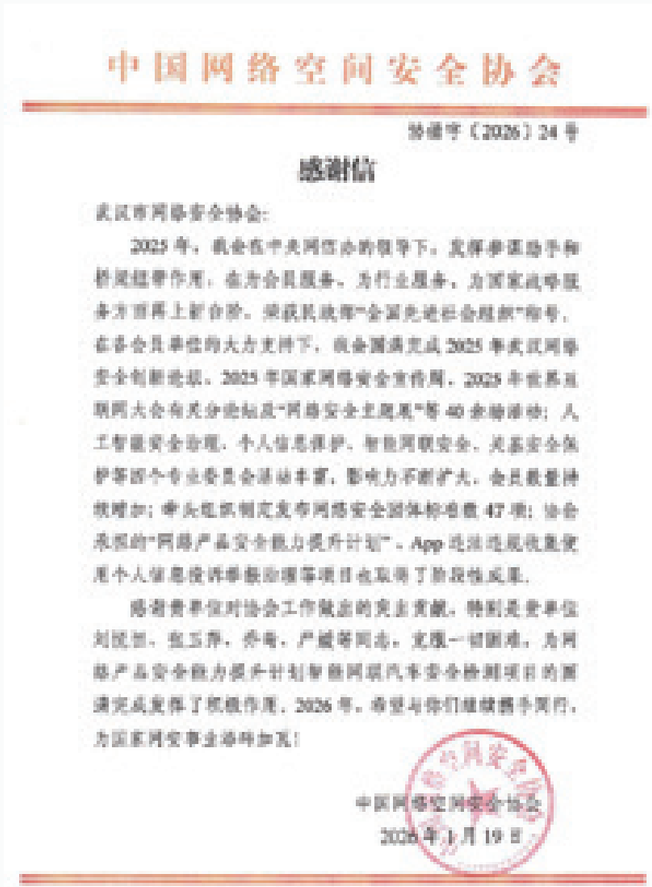


我会收到中国网络空间安全协会感谢信

近日，武汉市网络安全协会收到中国网络空间安全协会发来的感谢信，对协会在2025年度网络安全重点工作中作出的突出贡献予以充分肯定与表彰。

感谢信特别提及，武汉市网络安全协会秘书处相关同志攻坚克难，为网络产品安全能力提升计划 —— 智能网联汽车安全检测项目的圆满完成发挥了积极作用。

2026年，武汉市网络安全协会将以此为激励，持续深化行业协同，与全国同行携手共进，为国家网络安全事业高质量发展贡献力量。



中国网络空间安全协会

协通字〔2026〕24号

感谢信

武汉市网络安全协会：

2025年，我会在中央网信办的领导下，发挥桥梁纽带手和桥梁纽带作用，当好会员服务、为行业服务、为国家战略服务方面再上新台阶，荣获民政部“全国先进社会组织”称号，在各会员单位的大力支持下，我会圆满完成2025年度网络安全创新论坛、2025年国家网络安全宣传周、2025年世界互联网大会有关分论坛及“网络安全主题展”等40余场活动；人工智能安全治理、个人信息保护、智能网联安全、关基安全保护等四个专业委员会活动丰富，影响力不断扩大，会员数量持续增加；牵头组织制定发布网络安全团体标准数47项；协会承担的“网络产品安全能力提升计划”、App违法违规收集使用个人信息投诉举报处理等项目也取得了阶段性成果。

感谢贵单位对协会工作做出的突出贡献，特别是贵单位刘铭恒、张玉萍、乔琦、严威等同志，克服一切困难，为网络产品安全能力提升计划智能网联汽车安全检测项目的圆满完成发挥了积极作用。2026年，希望与你们继续携手同行，为国家网安事业添砖加瓦！

中国网络空间安全协会

2026年1月19日

我会协办的“湖北省‘51020’先进制造业集群产业生态之新型信息网络产业链专场活动”在汉举办

1月20日，湖北省“51020”先进制造业集群产业生态之新型信息网络产业链专场活动在武汉成功举办。省经信厅党组成员、副厅长刘良博出席并致辞，省通信管理局党组成员、副局长梁长岛出席活动。

活动聚焦6G前沿技术与产业融合，汇聚政府、企业、高校及金融机构，通过成果发布、主旨报告、产业推介与案例分享等多维环节，系统性展示了湖北在新型信息网络领域的前瞻布局与生态构建能力，为制造业高质量发展注入新动能。

活动上发布了一系列标志性重磅成果，集中展示了湖北在6G前沿领域整合资源、凝聚合力的系统性布局。活动现场，“湖北省6G创新发展联盟”正式启动组建。该联盟由中国信科集团、湖北电信、湖北移动、湖北联通、烽火通信、中信科移动共同发起，旨在汇聚产业与学术核心力量，协同攻关下一代通信关键技术与标准。同时，中国信科集团与湖北移动联合成立的6G技术及产业应用联合创新中心现场揭牌，武汉大学电子信息学院与中信科移动签署了6G联合实验室筹建合作协议，标志着以“产学研用”深度融合为特征的6G创新体系在湖北进入实质性推进阶段。

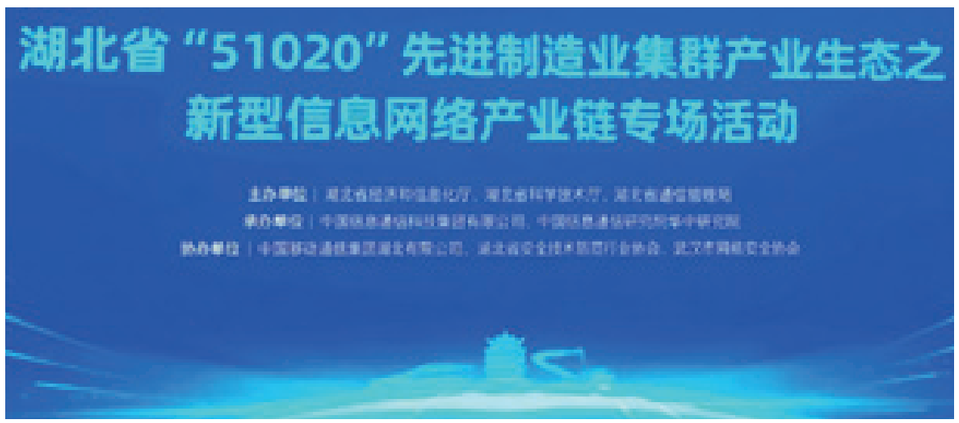


在主旨报告、产业推介与案例分享环节，活动实现了从技术前瞻、生态支撑到实践验证的全链条呈现。华中科技大学6G研究中心教授江涛所作的6G愿景与创新发展动向报告，深入剖析了技术趋势与产业机遇，为湖北抢占6G发展先机提供了学术洞察与路径参考。中信科移动、烽火通信介绍了前沿产品与解决方案，中国银行湖北省分行与人保财险公司分别阐述了金融支持产品与网络安全风险保障方案。湖北电信、移动、联通三家运营商分享了5G-A、工业互联网、AI等信息网络技术在多个工业场景的深度融合与创新应用案例。

为促进需求精准对接与产业链协同创新，本次活动特别举办了“6G及通信产业协同创新供需对接活动”，定向邀请了中国信科集团及电信运营商等产业链核心主体，就技术攻关、场景创新与网络建设等议题展开务实磋商，全力推动合作意向向具体项目转化。对接活动达成一系列的合作共识，产业链多方表示，将建立更加紧密的合作关系；将组建项目对接专班，定期磋商并向主管部门报送工作进展，为中信科早日“奋进千亿”贡献力量、更为我省“51020” 先进制造业集群发展添砖加瓦。

本次活动由省经信厅、省科技厅、省通信管理局联合主办，中国信科集团、中国信通院华中研究院承办，中国移动通信集团湖北有限公司、湖北省安全技术防范行业协会、武汉市网络安全协会协办。来自政府部门、企业、高校、科研机构、金融机构、行业协会及新闻媒体等200余名代表参加活动。



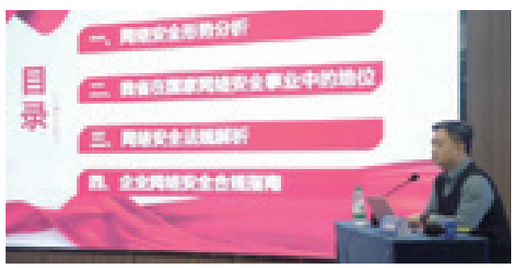


武汉市网络安全协会受邀为湖北交投高创监理公司专题培训授课

2026年1月27日，湖北交投高路公司旗下高创监理公司成功举办“向‘新’而行 以‘创’致远 打造高创监理创新策源地”主题培训。湖北省交通运输厅工程事务中心党委委员、总工程师卢柯，资质信用处处长周祖华，湖北交投高路公司党委书记、董事长李明，以及省交通建设监理检测协会秘书长邓志威出席活动。公司领导班子、各部门和项目负责人、技术骨干等共70余人参加培训。



卢柯在开班仪式上充分肯定了高创监理公司在数智化创新方面取得的阶段性成果，鼓励公司持续聚焦“育才强基、数智赋能、智慧领航”，争当行业创新发展的排头兵。李明对公司未来发展提出三点期望：一是坚持数智筑基，推动监理全流程数智化转型；二是推动协同聚力，深化产学研用合作；三是强化全局联动，营造人人参与的创新氛围。



本次培训聚焦“AI＋监理”、“智能装备”、“网络安全”等前沿领域，特邀武汉理工大学、石家庄铁道大学等高校学者，以及湖北省公路学会、武汉市网络安全协会、极视角科技有限公司等行业专家进行授课。作为受邀单位，我会秘书长刘悦恒同志以《以高水平安全保障企业高质量发展——工程监理行业网络安全合规解析》为题作专题授课。课程紧扣网络强国战略，结合工程领域典型案例，深入解析了《网络安全法》《数据安全法》等法规对监理行业的合规要求，系统阐述了构建“党委领导、管理驱动、技术防护、全员参与”综合防控体系的实践路径，并提供了具操作性的自查指南。网络安全是“一失万无”的底板工程，必须树立“时时放心不下”的责任意识，将安全要求深度融入监理全流程，为交通建设高质量发展筑牢安全屏障。授课内容扎实，针对性强，获得与会人员一致好评。

高创监理公司作为湖北交投高路公司旗下的专业力量，近年来持续加大研发投入，已累计取得知识产权成果40余项，多项技术在全国性行业会议中展示，形成了具有影响力的技术储备。

此次培训是推动智慧监理转型、促进行业高质量发展的一次重要实践。武汉市网络安全协会将持续发挥专业优势，深化与各行业的交流协作，共同为提升关键基础设施领域的网络安全防护能力贡献力量。

武汉市网络安全协会组织召开网络安全“双安认定”团体标准编制推进会

为深入贯彻网络强国战略，服务国家网络安全人才与创新基地建设，厘清产业边界、夯实发展基础，武汉市网络安全协会于近日在市委网信办会议室组织召开《网络安全企业认定规范》《网络安全产品和服务认定规范》两项团体标准编制推进研讨会。此次会议旨在系统推进“网络安全企业认定”与“网络安全产品及服务认定”（合称“双安认定”）工作，该项工作已纳入协会2026年度重点任务，是深化产业协同、构建标准体系的关键举措。

会议聚焦两项标准的编制背景、框架设计、任务分工及实施路径进行了务实研讨。与会代表一致认为，“双安认定”工作的开展对于科学界定产业范畴、引导行业规范发展、增强专业服务能力具有重要支撑作用，是推动我市网络安全产业高质量发展的重要基础性工作。

武汉市企业科技创新服务中心、武汉市计量标准质量研究院、武汉大学、武汉轻工大学等多所高校院所以及武汉安天、奇安信、绿盟科技、安恒信息、启明星辰、深信服、中国电信武汉分公司、黄鹤实验室、中金数据、德发电子、光谷信息等二十余家产业链相关单位代表积极参与讨论，并提出建设性意见。

本次会议标志着“双安认定”标准编制工作进入协同推进的新阶段。下一步，协会将充分吸纳各方智慧，加快完善标准内容，推动认定工作早日落地见效，为我市打造网络安全人才、创新、产业、供给和生态高地提供有力支撑。



武汉市网络安全协会走访慰问会员单位并致以新春感谢

值此新春佳节来临之际，为深化行业协作、凝聚发展共识，武汉市网络安全协会秘书处近期对部分会员单位开展调研走访活动，同时向各成员单位致以诚挚的节日问候，并对大家一年来为协会工作及武汉市网络安全事业发展所给予的宝贵支持表示衷心感谢。本次调研对象涵盖了协会副会长单位曙光网络科技有限公司，理事单位杭州迪普科技股份有限公司、中国移动通信集团湖北有限公司武汉分公司，以及湖北航天信息技术有限公司、武汉数安科技发展有限公司等会员单位。

副会长单位曙光网络科技有限公司是中科曙光控股的专注于工业数字化转型的科技企业，总部位于国家网安基地。此次调研，协会一行参观曙光科技位于基地的展厅，深入了解了该公司在算力及网络安全技术研发、行业实践方面的最新进展。作为协会核心成员，曙光网络展示了其作为行业引领者的技术积淀与责任担当，并表示将继续深度参与协会工作，协同各方力量，为武汉网络安全产业的高质量发展贡献关键支撑。双方围绕产业前沿动态、协同创新机制等议题进行了富有成效的探讨。

协会同期也与两家理事单位进行了交流。杭州迪普科技股份有限公司是国内信息安全产业的重要厂商之一。负责人重点向协会介绍了其在网络安全产品创新、解决方案构建及实战化安全服务方面的突出成果。中国移动通信集团湖北有限公司武汉分公司则分享了其在筑牢通信网络基础设施安全底座、保障城市数字化运行安全方面的系统性工作与重要经验。两家理事单位均表达了依托自身专业优势，积极通过协会平台促进技术共享与产业联动的明确意愿。

此外，协会还走访了会员单位武汉数安科技发展有限公司与湖北航天信息技术有限公司。武汉数安科技发展有限公司是武汉大数据产业发展有限公司与奇安信集团合资设立的国有控股企业，专注数据安全与信息技术服务，深度服务数字政府、数字城市建设等关键场景。湖北航天信息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。两家会员单位期待借助协会的桥梁作用，与更广泛的业界伙伴深化合作，共同推动细分领域的技术进步与方案落地。

通过此次系列走访活动，协会有效搭建了与各层级会员单位之间紧密沟通的渠道，精准掌握了不同领域企业的运行状况与发展诉求。各方普遍认为，在当前网络安全形势日益复杂的大背景下，进一步强化行业内部的凝聚力、促进资源整合与能力互补具有重要意义。

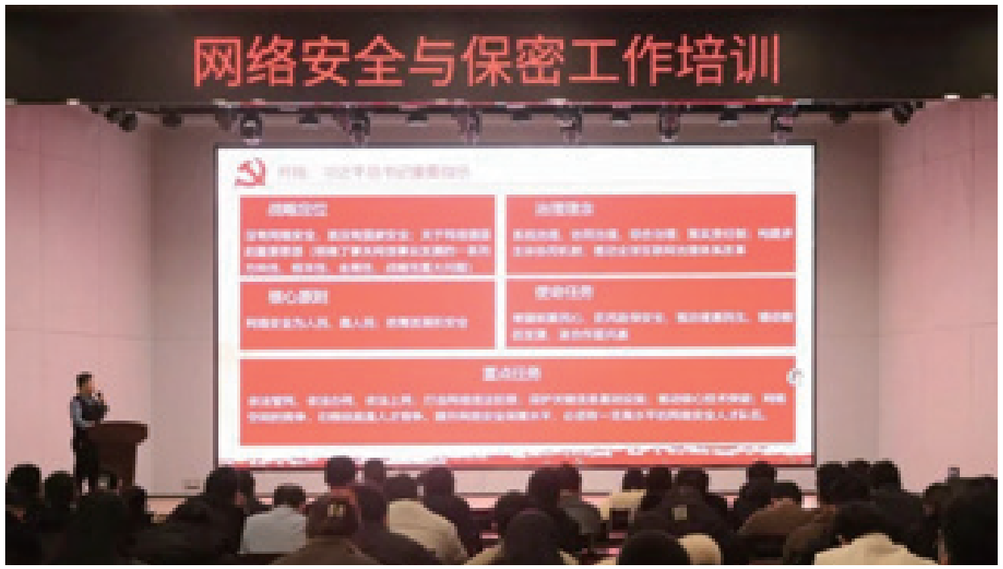
新的一年，武汉市网络安全协会将继续秉持“服务会员、推动行业、保障安全”的宗旨，持续优化工作机制，丰富服务内容，携手全体会员单位，共同构建更为牢固的网络安全防线，为推动武汉市数字经济社会高质量发展贡献力量。再祝各会员单位新春愉快、事业昌隆！

武网安协赴汉阳市政汇科智创开展工程行业网络安全合规专题培训

为筑牢工程行业网络安全防线，助力企业数字化转型安全发展，近日，武汉市网络安全协会党支部书记、秘书长、高级工程师刘悦恒，受邀赴会员单位汉阳市政集团汇科智创公司，开展“以高水平安全保障企业高质量发展——工程行业网络安全合规解析”专题培训，公司全体员工参加。

培训紧扣市政行业数字化安全核心需求，以习近平总书记关于网络安全工作的重要指示精神为指引，强调网络安全是关乎企业发展的战略问题，更是必须扛起的政治和法律责任。培训从网络安全形势分析、武汉在国家网络安全事业中的地位、网络安全法规解析、企业网络安全合规指南四大板块展开，结合境外黑客攻击、工程领域数据泄露等典型案例，直观剖析当前网络安全的隐蔽性、扩散性风险，解读国家网络安全人才与创新基地建设成果及产业发展现状。

同时，培训系统梳理《网络安全法》《数据安全法》等核心法律法规，重点讲解2026年实施的新版《网络安全法》处罚升级要点，以及与员工密切相关的相关法律责任，明确市政工程企业作为关键信息基础设施运营者的法定义务。针对企业合规实操，培训提出构建“党委领导、管理驱动、技术防护、全员参与”的综合防控体系，分享网络安全防护实用方法，为企业落实安全管控提供清晰路径。



4·15 全民国家安全教育日
武汉市网络安全协会走进中国铁建港航局集团有限公司第六工程分公司

筑牢工程领域网络安全防线

【编者按】安全是发展的前提，发展是安全的保障。在第十一个全民国家安全教育日之际，深入普及网络安全知识、提升重点行业合规防护能力，是协会践行社会责任、服务产业发展的应有之义。我会充分发挥专业优势与行业纽带作用，送服务进企业，围绕法规要求、风险防控、实操方法开展专题培训与答疑交流，助力工程建设企业夯实网络安全主体责任、提升合规治理水平。

4月15日，第十一个全民国家安全教育日当天，武汉市网络安全协会党支部书记、秘书长、高级工程师刘悦恒受邀走进中国铁建港航局集团有限公司第六工程分公司，围绕“统筹发展安全，护航‘十五五’新征程”主题，开展工程建设行业网络安全合规专题培训，助力企业以高水平网络安全保障高质量发展。

培训紧扣工程行业数字化转型实际，围绕网络安全形势、行业责任、法规解读、合规实操四大核心展开，兼具专业性与实操性。刘悦恒秘书长结合境外攻击、数据泄露等典型案例，剖析了BIM平台、智慧工地等场景安全风险，明确交通港航水利工程属国家关键信息基础设施重点保护领域，建议企业履行好系统防护、数据保护等法定责任。

培训重点解读了新修订《中华人民共和国网络安全法》处罚升级要点，阐释《数据安全法》等相关法规等相关条款，警示员工严守网络和数据安全底线。同时分享防护常识、自查方法等实操工具，指导企业落实等级保护、漏洞排查等关键措施，构建全方位安全防控体系。

培训后，六公司各部门负责同志与协会座谈交流，刘秘书长就企业提出的网络安全防护问题逐一解答，进一步巩固了培训成效。





4·15 全民国家安全教育日
——武汉市网络安全协会赴江汉大学开展专题交流活动

深化全民国家安全教育 助推产学研协同创新

为深入贯彻落实总体国家安全观，扎实推进第十一个全民国家安全教育日宣传教育工作，强化网络安全科普宣教实效，搭建校企产学研合作桥梁，2026年4月16日，武汉市网络安全协会组织协会会员单位、国家网络安全人才与创新基地产业联盟成员单位，走进江汉大学武汉市开源创新中心，开展网络安全专题科普宣讲暨校企对接交流活动。本次活动是协会全民国家安全教育日系列重点活动之一，紧扣国家安全宣传教育核心，兼顾科普育人与产业协同双重目标。



武汉大学国家网络安全学院博士万琳



活动伊始，武汉大学国家网络安全学院博士万琳，以《网络安全——筑牢数字空间的免疫屏障》为题，为江汉大学人工智能学院师生带来专业科普讲座。万琳博士围绕网络安全权威定义、常见网络攻击类型、数据泄露成因、核心防护措施及日常网络安全应对策略展开系统讲解，结合典型案例开展警示教育，并深入科普《网络安全法》相关内容，有效提升在校师生网络安全防范意识与法治观念，切实落实国家安全教育进校园的工作要求。

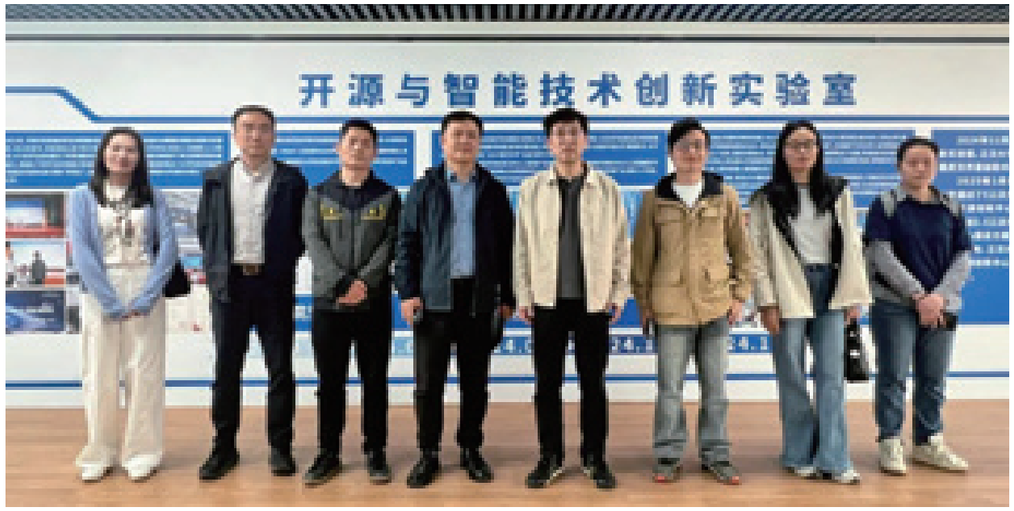
随后，江汉大学开源创新中心主任、人工智能学院副院长邓宏涛教授，带领各参会单位代表实地参观武汉市开源创新中心，详细介绍中心建设背景、运营宗旨、科研布局及产业服务成果。该中心作为武汉市开源体系重要创新平台，聚焦人工智能与开源技术研发、创新人才培养，为校企合作提供了坚实的科研与实践载体。



开源创新中心主任邓宏涛教授介绍实验室创新平台

参观结束后，协会牵头组织参会企业与学院、中心开展座谈交流。数字认证（武汉）有限责任公司、杭州帕拉迪网络科技有限公司、武汉市第三医院（协会医疗卫生与健康分会代表）等多家单位代表，围绕人才联合培养、技术协同攻关、科研成果转化、产业资源对接等议题深入探讨，达成多项初步合作共识。武汉市网络安全协会秘书长刘悦恒表示，协会将充分发挥平台纽带作用，持续助力会员单位交流协作，全力推动协会与各高校、会员单位间的产学研深度协同，凝聚行业发展合力。

此次活动，既是协会开展全民国家安全教育日的重要实践，充分发挥了网络安全科普宣教、筑牢国家安全思想防线的作用；也有效依托协会平台优势，深化了校企产学研用融合，为推动武汉网络安全领域人才链、创新链、产业链精准对接，助力区域网络安全产业高质量发展注入了新动力。



江汉大学开源创新中心

2025年4月，江汉大学获批武汉市开源创新中心（人工智能方向），该中心依托江汉大学人工智能学院与江汉大学开源创新中心开展建设，是武汉市开源体系建设的重要创新平台。中心坐落于江汉大学J31、J33教学实验楼，使用面积1000m2。中心以“开源开放、协同创新、赋能产业”为宗旨，围绕人工智能与开源技术开展技术研发、创新人才培养和产业服务，致力于打造具有示范意义的高校开源与人工智能技术创新基地。

中心建设基础来源于江汉大学与CSDN联合共建的“开源与智能技术创新实验室”。该实验室自2023年启动建设，通过校企合作整合高校教学科研资源与开发者社区生态，形成面向人工智能与开源技术的创新实验平台，并形成稳定的技术团队与运维团队，为开源创新中心提供了重要技术基础与人才支撑。

武汉市开源创新中心（人工智能方向）以人工智能开源生态为核心方向，面向教学、科研和产业应用开展人工智能技术创新和开源人才培养，服务武汉市人工智能产业发展。

武汉市网络安全协会第二届理事会第四次会长办公会顺利召开

为深入践行协会办会宗旨，持续提质增效、履职赋能，切实做实做细服务会员、衔接政府、赋能社会各项核心工作，全力助推武汉网络安全产业高质量发展，4月23日，武汉市网络安全协会第二届理事会第四次会长办公会在协会汉口办公点顺利召开。协会会长、副会长、监事单位代表及秘书处全体工作人员参会。

会议坚持以习近平新时代中国特色社会主义思想为指导，深入学习贯彻习近平总书记关于网络强国的重要思想，集体学习了中央、省、市网信办主任工作会议精神和市委网信办工作要求。会议强调，协会将立足武汉国家网络安全人才与创新基地核心承载区优势，主动服务“中国网谷”建设大局，紧密对接各级网信主管部门，强化行业协同与资源整合，为加快推进网络安全体系和能力现代化、服务武汉网信事业高质量发展贡献坚实力量。



会议全面复盘协会阶段性工作开展情况，系统听取近期重点工作专项汇报，集中审议2026年度整体工作规划及重点任务部署等核心事项。与会人员围绕协会内部治理提质、运营管理标准化建设、年度重点工作落地推进等关键议题开展深度研讨、充分交流磋商，形成统一工作决议。本次会议进一步完善了协会规范化运行机制，明确了全年工作推进路径，为协会年度各项工作落地见效、实现规范化、专业化、高质量发展筑牢坚实基础。

会议聚焦产业协同发展，专题研究部署协会联动国家网络安全人才与创新基地产业联盟2026年度重点工作。会议明确，协会本年度将立足武汉网络安全产业发展大局，锚定完善产业生态、精准赋能企业、提质人才引育、规范行业秩序、擦亮行业品牌五大核心方向，持续迭代升级行业服务体系、丰富服务供给内容。充分发挥行业协会平台聚合优势，整合产业资源、凝聚发展合力，持续优化武汉网络安全产业发展生态，稳步提升区域网络安全产业核心能级与综合竞争力。

会议统筹谋划、细化部署协会第二届第三次会员大会各项筹备工作，对会议流程、会务安排、工作衔接等事项进行系统化、精细化统筹安排，全力保障会员大会规范严谨、平稳有序、高效圆满召开。同时，会议围绕强化分支机构协同联动、拓宽行业服务覆盖面、深化跨区域行业交流协作、搭建多元合作平台等重点工作展开深入研讨。各参会单位立足行业发展实际、结合自身资源优势积极建言献策，纷纷表示将坚决落实协会各项工作部署，密切协同配合、主动担当作为，共同助力武汉网络安全行业提质升级、高质量发展。

此次会长办公会的召开，有效统一了行业思想、凝聚了产业发展共识，清晰划定了协会2026年度工作主线、明确了重点攻坚方向。下一步，武汉市网络安全协会将以本次会议精神为统领，紧扣全市网络安全和信息化工作总体部署，坚守初心使命、聚焦主责主业，持续夯实内部建设、提升专业服务能力。充分发挥政企桥梁、行业纽带、产业赋能核心作用，深耕行业服务、聚力产业赋能，持续为武汉网络安全产业创新迭代、全市网络安全保障体系和能力现代化建设贡献坚实行业力量。

武网安协召开《网络安全企业认定规范》《网络安全产品和服务认定规范》团体标准编制委员会第二次全体会议

4月23日，《网络安全企业认定规范》《网络安全产品和服务认定规范》团体标准编制委员会第二次全体会议在武汉市企业科技创新服务中心顺利召开。本次会议全体标准编制参与单位及相关人员参会，会议聚焦标准条款优化完善、合规性与实操性全面提升，对团体标准编制下一阶段核心工作作出系统部署。

会上，标准编制工作组首先就两项团体标准前期编制进展、初稿核心内容、行业调研成果及前期征集的各方意见建议汇总情况，向全体参会人员作了全面详细汇报。随后，全体参会人员围绕标准现有条款开展集中研讨，重点聚焦标准内容的合规性、实际应用的可行性、条款表述的严谨性三大核心维度，对编制过程中存在争议的内容逐一梳理、逐条论证、充分研讨，最终形成了统一的调整优化方向。会议进一步细化明确了各参编单位的后续修改任务、责任分工与完成时限，系统梳理了标准编制需补充完善的各类支撑材料，确保各项编制工作闭环推进、落地见效。最后，编制工作组负责人对本次会议成果进行了全面总结，统筹部署了下一阶段团体标准编制的整体工作安排。

下一步，武汉市网络安全协会将牵头标准编制工作组，严格按照会议要求加快标准条款修改完善，持续广泛吸纳行业各方合理意见，不断提升标准的科学性、合规性与实操性，力争两项团体标准早日发布实施，为国家网络安全人才与创新基地建设、数字武汉高质量发展提供坚实的标准支撑与安全保障。

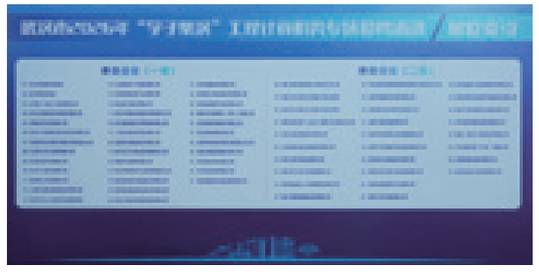


“学子聚汉”工程计算机类专场招聘活动顺利举办

【编者按】人才是产业发展的核心底气，助力青年人才留汉就业、服务产业人才需求，是协会的职责所在。为扎实推进“学子聚汉"工程，精准匹配计算机与网络安全领域人才供需，我会充分发挥行业纽带作用，联合武汉市人才服务中心共同打造专场招聘品牌活动，为高校毕业生与行业企业搭建面对面对接桥梁。

为深入贯彻落实党中央、国务院和省、市关于高校毕业生就业创业工作的决策部署，扎实推进“学子聚汉”工程，精准搭建计算机领域高校毕业生与用人单位对接平台，4月30日，武汉市2026年“学子聚汉”工程计算机类专场招聘活动在武汉人才之家顺利举办。本次活动以“就在武汉创赢未来”为主题，由武汉市人力资源和社会保障局、武汉人才集团主办，武汉市人才服务中心承办，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟等单位协办，有效推动计算机领域人才供需精准匹配，助力高校毕业生实现高质量就业。





优质企业齐聚一堂 产业覆盖全面多元

本次专场招聘聚焦计算机、网络安全、人工智能、软件信息、智能制造等核心领域，吸引湖北珞珈实验室、科大讯飞、众创网、湖北东方网盾、绿盟科技、武汉安域、武汉德发电子、武汉华康等60余家行业优质企事业单位参会，涵盖高端科研平台、网络安全龙头企业、软件信息领军企业、人工智能新锐公司、智能制造骨干企业等多元主体，形成覆盖计算机全产业链的招聘矩阵。

参会企业聚焦武汉数字经济与网络安全产业发展需求。精准对接高校计算机类、网络空间安全类、电子信息类等专业毕业生，充分体现了我市网信产业对青年人才的迫切需求，为毕业生提供了多元化、高层次的就业选择。



优质岗位精准供给 贴合应届求职需求

活动现场，参会企业集中发布两百余个优质岗位，岗位设置紧扣高校应届毕业生特点。以技术研发类岗位为核心，同步设置综合管理、见习实践、市场运营等配套岗位，全面降低工作经验门槛，重点面向 2026 届本硕博毕业生。

岗位类型涵盖算法工程师、嵌入式开发工程师、Java开发工程师、FPGA工程师、AI开发工程师、网络安全工程师、渗透测试工程师、等保测评工程师等核心技术岗位，同时设置适配应届生的实践型实习岗位。既满足企业技术研发需求，也为应届毕业生提供了从校园到职场的平稳过渡通道，充分契合计算机专业人才培养方向与就业期待。



供需对接高效顺畅 就业服务精准贴心

活动现场人头攒动、氛围热烈，众多计算机类高校毕业生携带简历有序入场，与企业招聘负责人面对面交流，详细咨询岗位职责、发展路径、薪酬福利、留汉政策等问题。多家企业为吸引人才留汉发展推出五险一金、人才公寓、一对一导师带教、核心项目参与、系统化技能培训等配套保障，切实解决毕业生就业后顾之忧。

活动同步设置政策咨询服务台，现场宣讲“学子聚汉”人才政策、高校毕业生就业创业扶持、人才落户、住房补贴等利好政策。为毕业生提供一站式政策解读与就业指导服务，进一步提升求职对接效率与服务体验。



深化产才融合对接 持续汇聚青年英才

本次计算机类专场招聘活动，是我市稳就业、聚人才、促发展的重要举措，有效打通了计算机领域人才“培养、引进、对接、就业”全链条，为武汉数字经济、网络安全产业高质量发展储备了青年人才力量。

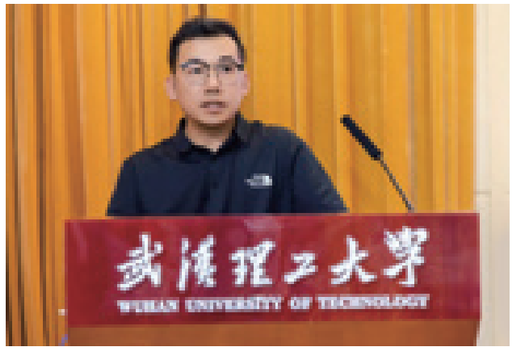
作为联合组织单位武汉市网络安全协会、国家网络安全人才与创新基地产业联盟充分发挥行业桥梁纽带作用，联动优质企业、整合岗位资源，推动人才供给与产业需求精准适配。下一步，我市将持续深化“学子聚汉”工程，常态化开展分领域、分专业专场招聘活动，不断优化人才服务体系，吸引更多高校毕业生留汉就业创业，为武汉打造国家网络安全人才与创新高地、建设全国科技创新中心提供坚实人才支撑。

喜获省级认证！
我会知识产权人才队伍再壮大 服务能力迈上新台阶

近日，2026年全省知识产权专员考核认证培训在湖北省知识产权（武汉）基地顺利举办。本次培训由湖北省知识产权局组织，前期线上培训覆盖全省17个市州11712名企业代表，累计学习回看超20万人次，本次遴选800名优秀学员开展线下考核认证，着力提升知识产权专员实操能力，以知识产权服务赋能产业高质量发展。



本次认证考核中，我会多名职工顺利通过评审评定，成功考取湖北省知识产权专员认证资质，充分彰显了协会知识产权人才队伍过硬的综合素养与专业能力。我会秘书处科研部负责人乔奇受邀参训，立足网络安全产业发展实际，现场分享《深耕网安知识产权服务 赋能国家网安基地产业创新发展》典型案例；围绕知识产权创造、运用、保护、管理全流程分享实战经验，推介可借鉴、可复制的工作路径与实操方法，切实助力参训学员提升专业实务能力。

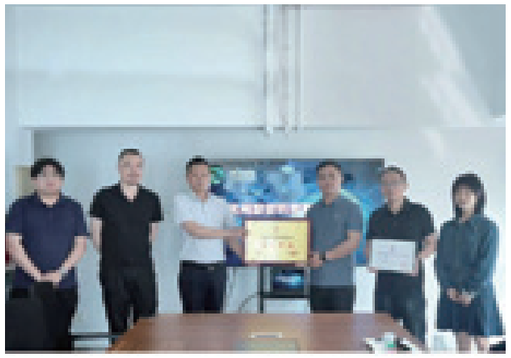


培训期间，乔奇全程认真参训、积极交流研讨，凭借突出表现与优异成绩，获评2026年全省知识产权专员认证培训班“优秀专员”。本次培训同步挖掘推广优秀典型案例、落实人才激励政策，优秀专员将优先推荐参与国家和省级人才选拔评定。

此次多名职工通过省级知识产权专员认证，标志着我会知识产权服务专业能力进一步提升，服务体系与人才支撑更趋完善。下一步，协会将以此次培训为契机，持续深耕网络安全领域知识产权服务，发挥优秀人才典型示范作用，推动知识产权与网安产业深度融合，精准助力国家网安基地产业联盟及入驻企业创新升级，深耕赋能我市网安产业、激活高质量发展持久新势能。

默安科技：
以AI驱动主动防御 筑牢数字安全坚实屏障

近日，武汉市网络安全协会秘书处一行赴杭州默安科技有限公司武汉分公司走访交流。默安科技武汉分公司负责人黄超携团队热情接待，并向协会一行详细介绍企业发展历程、核心技术与区域布局情况。协会现场为企业正式授予武汉市网络安全协会会员单位证书与牌匾，双方就技术创新、产业发展、生态共建等议题深入交流并达成合作共识。





默安科技成立于2016年，是国内领先的技术型主动防御安全厂商、国家级专精特新重点 “小巨人”企业。公司核心团队源自阿里云安全核心团队，骨干成员拥有20余年网络攻防实战与重大安全项目建设经验，是国内主动防御领域的标杆力量。企业以人工智能为核心驱动力，专注构建实战化智能主动防御体系，业务涵盖智慧运营安全、左移开发安全、软件供应链安全、云与云原生安全四大领域，通过AI赋能的安全产品与专业化服务，为客户提供全生命周期安全风险管控，助力客户打造智能化、体系化、常态化安全运营能力。

截至目前，默安科技已完成近6亿元融资，建有省级高新技术企业研发中心、工信部重点实验室电力分中心、农业农机分中心等创新平台，拥有40余项专利、50 余项软件著作权，深度参与 10 余项国家及行业网络安全标准制定，技术实力与行业影响力稳居国内前列。

默安科技武汉分公司于2021年3月成立，是企业布局华中区域的核心战略支点，内设研发中心与华中安服中心，立足武汉、服务全省、辐射中部。凭借过硬的技术实力与优质的服务水平，分公司先后获得湖北省通信管理局、湖北省网络与信息安全通报中心等监管部门授予的技术支撑单位资格，成为湖北区域网络安全保障的重要力量。分公司聚焦政府、央国企、金融、高校等关键领域，为省内几十家重点行业客户提供专业网络安全支撑，在湖北省“铸网行动”“护网行动”等重大网络安全保障工作中表现突出，为湖北网络安全防护体系建设作出积极贡献。

武汉市网络安全协会秘书长刘悦恒对默安科技加入协会表示热烈祝贺，充分肯定企业深耕技术创新、扎根武汉服务地方的发展举措，认为企业的加入进一步壮大了协会会员队伍，为武汉网络安全产业发展注入新动能。秘书长指出，依托武汉“五谷丰登”产业布局与“中国网谷”建设契机，协会将充分发挥桥梁纽带作用，聚焦人才服务、产业对接、活动支撑、品牌推广等方面，为会员单位提供精准化、全方位服务，助力企业高质量发展。

交流中，双方就深化合作、资源共享、活动共办、品牌共建达成一致意向。未来，武汉市网络安全协会将为默安科技搭建宣传展示、政策对接、业务合作的优质平台；默安科技将持续加大在汉投入，深化校企合作、拓展行业应用，充分发挥AI主动防御技术优势，积极参与行业交流、攻防演练、安全宣传等工作，与协会及各会员单位携手共进，共同推动武汉网络安全产业提质增效、做大做强，为华中地区数字经济健康发展筑牢坚实安全屏障。



公司介绍

杭州默安科技有限公司成立于2016年，是一家专注于网络安全、云安全软件研发与服务的技术驱动型安全企业，国家级专精特新重点小巨人企业、中国网安产业竞争力50强、中国软件和信息技术服务名牌企业;建有省级高新技术企业研究开发中心、工信部重点实验室电力分中心及农业农机分中心。

公司以人工智能赋能主动防御，为能源、交通、制造、通信、政府、金融等重要行业的2000余家客户提供安全保障，常年支撑中央网信办、公安部、工信部、证监会的漏洞挖掘、攻防演练、威胁情报、软件供应链检查、云安全检查等专项工作，参与制定国家、行业等标准10余项;参与包括G20峰会、建党百年、北京冬奥会、杭州亚运会等多项重大活动网络安全保障任务。

赋能产业· 精准惠企
武汉科创政策宣贯助力网安与AI产业高质量发展

近日，“赋能产业，精准惠企”科技创新政策宣贯会在武汉市东西湖区国家网络安全人才与创新基地网安软件园顺利举办。本次活动由武汉市网络安全协会、国家网络安全人才与创新基地产业联盟主办，武汉市科创局企业科技创新服务中心提供支持，华中科技大学国家大学科技园网谷分园承办，全市各领域科创企业、高校师生创业团队、AI创新主体代表参会。

活动聚焦网络安全、数字经济、人工智能等产业发展需求，系统解读全市科创梯度培育、AI创新、算力金融等最新惠企政策，精准对接企业发展痛点难点，打通政策落地“最后一公里”，助力辖区科创主体提质增效、稳健发展。本次宣贯会采用“政策权威解读＋科技金融宣讲＋现场答疑对接”的标准化服务模式，全面覆盖科技企业种子期、初创期、成长期、成熟期全生命周期培育体系。宣讲内容紧扣当前产业培育重点，系统涵盖初创企业育苗、中小微孵化培育、高新技术企业梯度跃升、人工智能OPC创新培育、孵化载体提质增效、科创金融精准支撑等核心板块。精准适配不同层级、不同赛道科创企业的发展与申报需求，实现政策宣讲精准触达、资源对接高效落地。

会上，武汉市科创局企业中心相关工作人员对武汉市科创企业全梯度培育体系作系统解读。针对初创科创主体，宣讲重点解读了高校师生创新创业专项扶持政策，明确了初创企业入库培育标准、申报方式及遴选程序；详细介绍了教师“青苗计划”、大学生创新创业项目扶持、毕业生一次性创业补贴、岗位社保补贴等实操举措，进一步畅通高校科技成果转化、师生创业落地孵化通道。

围绕人工智能产业新赛道培育，本次活动重点解读武汉市人工智能OPC创新发展“汉十条”政策。宣讲围绕算力、数据、模型、人才、场景、金融等核心要素，系统阐释OPC新型创新创业主体培育路径。一是强化算力服务，依托市级算力公共服务平台发放算力券，补贴企业算力使用成本；二是畅通数据供给，依托“汉数通”开放公共与行业数据集，对优质数据研发项目享受专项补助；三是扶持模型研发，对AI模型研发、采购分别予以经费补贴；四是完善人才引育，通过校企合作、技能培训、安居及购房补贴集聚AI复合型人才；五是建设OPC生态社区，择优给予建设资金扶持；六是落地创业启动资助，对优质初创OPC拨付专项创业资金；七是搭建线上开放平台，上线AI商城、实训板块，面向大学生发放产品体验券；八是开放应用场景资源，常态化发布场景清单，落地示范项目资金扶持；九是强化科创金融保障，配套创业担保贷、算力专项贷、风险补偿等政策；十是营造产业氛围，常态化举办OPC创新创业赛事与行业沙龙。





针对成长型科创企业，宣讲全面梳理科技型中小企业、小微高企跃升、骨干高企瞪羚培育四大政策体系。其中，科技型中小企业可享受研发费用加计扣除、亏损结转年限延长等税收红利；宣讲清晰界定高新技术企业研发投入占比、知识产权、高新产品营收等核心认定指标及分级奖励标准；针对小微高企，明确市级研发中心备案“免申即享”后补助机制；对瞪羚企业，按照营收规模、增长速度实施梯度遴选，配套股权投资、专项扶持等培育资源，推动企业持续迭代跃升。

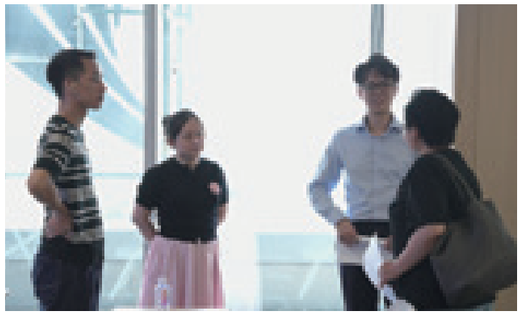


中国银行湖北分行科技金融中心杨林蔚围绕中银科创＋综合服务体系开展分享。依托该行省市县多级专业化网点布局，介绍覆盖企业从初创到成熟全生命周期综合金融方案，重点结合网安、AI行业特点，详解算力贷、知识价值信用贷、科创普惠贷、股权投资等特色产品，依托绿色审批通道与政银风险分担机制，切实缓解科创企业融资难题。



宣讲结束后，活动设置现场互动答疑环节。参会企业代表围绕算力券申领、高企研发费用归集、孵化器绩效申报、科创贷款办理流程等实务问题集中提问。现场专家逐一答疑解惑，精准纠正申报误区、明晰适配条件、梳理办理路径，切实解决企业实际困难。

本次政策宣贯会立足武汉数字经济与网络安全产业发展实际，以企业需求为导向，实现政策解读精细化、金融赋能专属化、对接服务场景化，有效打通政企银信息壁垒，进一步提升科创政策知晓率、申报率和落地转化率。下一步，武汉市网络安全协会将携手国家网安基地产业联盟持续聚焦重点产业赛道，常态化开展系列服务活动，持续完善科技企业全生命周期培育体系，不断优化区域创新创业营商环境，为武汉科创产业集群高质量发展、新质生产力加速培育提供有力支撑。



精准赋能专技人才 助力产业提质升级

2026年度电子信息与通信工程职称申报专场培训会顺利举办

6月22日下午，由武汉市网络安全协会主办，武汉市人才服务中心提供支持的2026年度电子信息与通信工程系列职称申报专场培训会，在武汉人才之家顺利举办。我会部分会员、全市网络安全领域专精特新企业、高新技术企业的相关负责人及专业技术骨干到场参训。

本次培训聚焦行业专技人才发展诉求，紧扣职称申报工作中的痛点难点，精准开展针对性辅导。培训系统解读2026年度职称申报政策细则，梳理申报全流程操作规范。同时，协会人才服务部负责人现场演示职称申报线上系统完整填报流程，细致讲解纸质材料整理、内容编撰、材料提报等关键环节的核心要点与注意事项。培训设置答疑交流环节，现场氛围活跃，参会人员围绕申报工作中的实际问题主动提问、深入交流，为高效推进本年度职称申报工作夯实基础。

培训结束后，参训人员纷纷表示，本次培训内容紧贴申报工作实际、实用性突出，有效解答了职称申报过程中的各类疑惑，帮助大家更加全面、透彻地掌握职称申报相关政策与实操方法。参会企业人力资源负责人表示，本次培训内容扎实、指导性强，既厘清了现阶段的申报工作思路，也为企业常态化开展人才培养、统筹员工职业晋升、完善内部人才发展体系提供了有力支撑。

人才队伍建设是产业稳步发展的重要保障，扎实开展专技人才服务工作，能够有效助力技术人才成长，夯实产业人才储备。下一步，武汉市网络安全协会将立足产业发展实际与企业人才需求，持续优化行业人才服务举措，助力产业人才队伍提质扩容，为区域数字经济产业发展筑牢人才保障。

本次活动主题鲜明、内容扎实，有效推动了基层党建与业务工作的深度融合。双方表示将持续深化合作，切实将党建活力转化为发展动力。



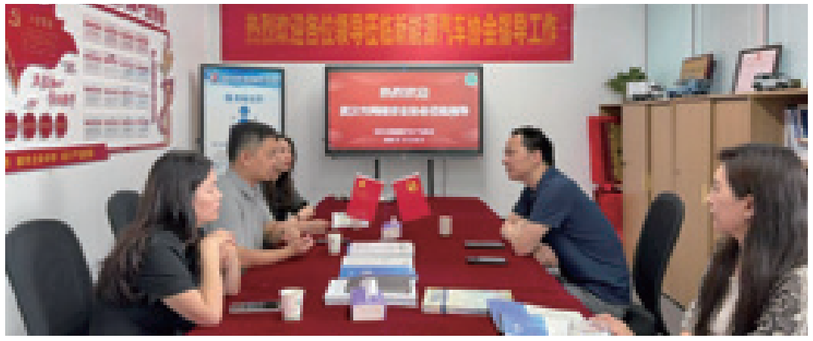
武汉市网络安全协会走访武汉市新能源汽车产业协会

深化跨界协同 共筑产业安全

6月25日，武汉市网络安全协会党支部书记、秘书长刘悦恒率秘书处一行，赴武汉市新能源汽车产业协会开展联谊走访。双方以深化智能网联汽车安全领域协同、助力武汉车谷网谷协同发展为主题举行专题座谈，共商产业融合发展路径。武汉市新能源汽车产业协会执行会长师广友和秘书长韩昕洋热情接待。

座谈期间，双方分别介绍了协会发展概况、行业资源布局与核心工作开展情况，坦诚互通新能源汽车与网络安全产业的发展现状及协作需求，围绕智能网联汽车安全建设、武汉“中国车谷”与“中国网谷”联动发展、落实“五谷丰登”发展战略等议题深入交换意见。双方就联合开展产业对接、共建标准、深化产学研协同合作等事项进行了沟通，明确了后续合作对接的工作机制与推进方向。

本次活动主题鲜明、内容扎实，有效推动了基层党建与业务工作的深度融合。双方表示将持续深化合作，切实将党建活力转化为发展动力。





「教育数智化安全治理专栏」



“数智问道 智护校园安澜”
教育数智化安全治理主题活动圆满举行

近日，以“数智问道 智护校园安澜：教育数智化安全治理”为主题的教育行业专题活动在武汉临空港会展酒店金银湖厅圆满举行。本次活动由湖北大数据集团数字科技有限公司、武汉吧哒科技股份有限公司、中国电信武汉分公司联合主办，武汉市网络安全协会携手东湖数据安全创新联盟、国家网络安全人才与创新基地产业联盟共同承办。来自全省教育主管部门、47所高校、科研院所及网络安全领域的百余位专家学者、行业代表齐聚一堂，共商教育数智化转型大计，共探校园安全治理新路径。会议由武汉纺织大学信息化工作办公室主任陈建、中国地质大学（武汉）信息化工作办公室副主任宋焘共同主持。





活动开始，湖北省教育厅信息化发展中心副主任翟培甫、东湖数据安全创新联盟专家委员会组长张屹教授先后致辞。致辞强调，教育数字化是教育现代化的核心引擎，数据安全与网络治理是教育数字化转型行稳致远的底线保障。希望通过本次活动搭建政校企协同交流平台，凝聚多方智慧与力量，共同构建安全可控、高效便捷、智慧创新的教育数字新生态。

主旨报告环节，教育部教育管理信息中心网络安全处杨伟平处长作权威政策解读，系统阐释《教育数据分类分级指南》。他从工作背景、核心内容、典型案例、编制过程、下一步计划及近期工作思考等多个维度进行深入讲解，明确了教育数据安全治理的核心框架与实施规范，为各级各类学校健全数据安全体系、强化风险防范能力、落实监管责任要求提供了精准指引和实操遵循，为教育系统数据安全工作指明方向。

据安全体系、强化风险防范能力、落实监管责任要求提精准指引和实操遵循，为教育系统数据安全工作指明方向。

随后，华中师范大学信息化办公室副主任唐亦非、湖北大学大数据中心主任陈昊、信息支援部队工程大学教授何俊、湖南师范大学数据与信息化建设管理处副处长张智勇、湖北国土资源职业学院信息中心主任侯文平依次作主题分享，分别从高校数字化转型实践、云网安一体化管理、实战为不同类型院校的校园安全治理提供了可复制、可推广的实践方案。

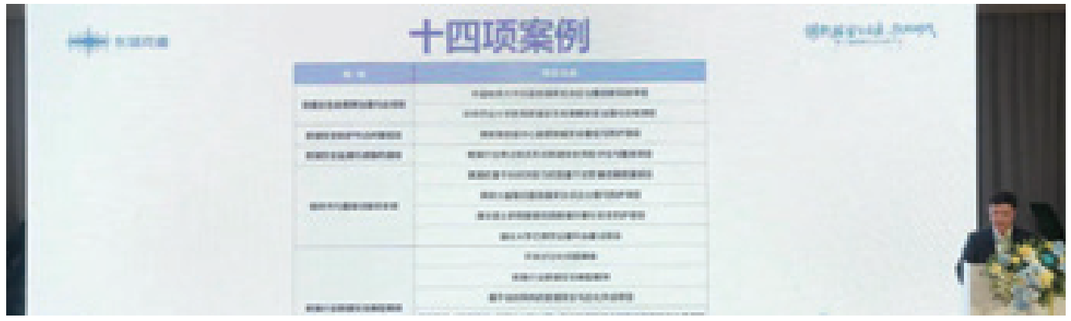


论坛现场，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟联合发布了《教育行业数据安全典型案例集》。武汉市网络安全协会、国家网络安全人才与创新基地产业联盟秘书长刘悦恒出席发布仪式并作介绍。

该案例汇聚了中国地质大学（武汉）、华中农业大学、湖北大学、武汉学院等高校，以及中国电信武汉分公司、武汉安域信息安全技术有限公司、武汉通达数据科技有限公司、杭州安恒信息技术有限公司、星融元数据技术有限公司、宏杉科技等企业的一线实践，分为数据全生命周期治理与合规、数据安全防护与访问管控、数据安全监测与威胁防御、新技术与基础设施安全、教育行业数据安全典型案例五大板块，覆盖数据分类分级、敏感信息管控、考试系统防护、量子加密通信、云网安一体化、信创架构升级、人脸数据安全中台等教育行业高频场景，为各类教育机构提供可复制、可推广的数据安全治理“实操手册”。







类别	项目名称	单位
数据全生命周期治理与合规类	中国地质大学校园数据安全综合治理创新实践项目	中国地质大学（武汉）信息化工作办公室
	华中农业大学教育数据全生命周期安全治理与合规项目	华中农业大学
数据安全防护与访问管控类	某教育数据中心敏感数据安全管控与防护项目	武汉通达数据科技有限公司
数据安全监测与威胁防御类	教育行业考试报名系统数据安全风险评估与整改项目	武汉安域信息安全技术有限公司
新技术与基础设施安全类	某高校量子科技创新及校园量子加密通信网搭建项目	中国电信股份有限公司武汉分公司
	某财大智慧校园数据安全综合治理与防护项目	杭州安恒信息技术股份有限公司
	湖北国土职院智慧校园数据共享与安全防护项目	湖北国土资源职业技术学院
	湖北大学云网安运管平台建设项目	湖北大学
教育行业数据安全典型案例	开放式云化校园网络	星融元数据技术有限公司
	教育行业数据安全典型案例	湖北某省属“双一流”高校
	基于信创架构的数据安全与云化升级项目	某省属重点高等院校
	高校基于“态势感知+数据中心防火墙”的内网横向攻击隔离与数据安全治理项目	湖北大学知行学院
	人脸数据安全中台教育数据安全案例	武汉学院
	面向数智化校园基础设施解决方案	宏杉科技

在圆桌研讨环节，中南民族大学信息化建设管理处处长张淼担任主持人，来自武汉大学、中国地质大学（武汉）、海军工程大学、武汉城市职业学院、湖北邮电规划设计有限公司、武汉吧哒科技股份有限公司等单位的业务负责人，与企业代表围绕教育数智化安全治理的痛点难点、发展趋势及应对策略展开深入研讨，碰撞思想火花，凝聚行业共识，为推动教育行业安全高质量发展建言献策。

本次教育行业活动的成功举办，不仅搭建了教育行业数智化安全交流合作的重要平台，更推动了政策、技术、实践经验的深度融合。未来，武汉市网络安全协会将充分发挥桥梁纽带作用，持续整合行业资源，深化政校企协同合作，不断完善教育行业网络安全服务体系，以数智技术赋能安全治理，共同守护校园数字安全，助力教育数字化高质量发展。



教育行业数据安全案例集

第一章 数据全生命周期治理与合规类

(一) 中国地质大学(武汉)信息化工作办公室
中国地质大学校园数据安全综合治理创新实践项目

(二) 华中农业大学
华中农业大学教育数据全生命周期安全治理与合规项目

(三) 湖北国土资源职业技术学院
湖北国土职院智慧校园数据共享与安全防护项目

(四) 湖北大学
湖北大学云网安运管平台建设项目

第二章 数据安全防护与访问管控类

(一) 武汉通达数据科技有限公司
某教育数据中心敏感数据安全管控与防护项目

第三章 数据安全监测与威胁防御类

(一) 武汉安域信息安全技术有限公司
教育行业考试报名系统数据安全风险评估与整改项目

第四章 新技术与基础设施安全类

(一) 中国电信股份有限公司武汉分公司
某高校量子科技创新及校园量子加密通信网搭建项目

(二) 杭州安恒信息技术股份有限公司
某财大智慧校园数据安全综合治理与防护项目

第五章 教育行业数据安全典型案例

(一) 星融元
开放式云化校园网络

(二) 湖北某省属“双一流”高校
教育行业数据安全典型案例

(三) 某省属重点高等院校
基于信创架构的数据安全与云化升级项目

(四) 湖北大学知行学院
高校基于“态势感知+数据中心防火墙”的内网横向攻击隔离与数据安全治理项目

(五) 武汉学院
人脸数据安全中台教育数据安全案例

(六) 宏杉科技
面向数智化校园基础设施解决方案

中国地质大学
校园数据安全综合治理创新实践项目

中国地质大学(武汉)信息化工作办公室

1 场景

针对高校数据资产体量庞大、共享需求频繁，但传统边界防护失效、全生命周期管控缺失的严峻痛点，我校曾长期面临数据底数不清、敏感信息明文存储、开发测试直连生产库、数据共享无法溯源等高风险挑战。为破解困局，我们坚持“管理+技术”双轮驱动，构建了覆盖数据全生命周期的场景化精准防护体系。通过自动梳理分类分级，动态匹配数据库防火墙、动静脱敏及访问控制策略，成功解决了敏感数据“权限不明、流转失控、责任难定”的核心难题。项目实施后，我校数据安全能力成熟度显著提升，实现核心数据100%脱敏、高危操作实时阻断及泄漏事件分钟级溯源，有效支撑了跨部门科研协作与数据共享，为教育行业提供了可复制、可推广的“地大样板”，具有显著的乘数效应。

2 成果呈现

2.1 整体逻辑架构

我校确立了“一中心、四体系、六过程”的数据安全顶层设计：坚持以数据安全为核心，构建组织、管理、技术、运营四大支撑体系，覆盖数据采集、传输、存储、处理、交换、销毁全生命周期六大关键环节，从而构筑起严密高效的数据安全治理框架。

(1) 管理架构(三权分立)：打破部门壁垒，建立由数据主管部门统筹决策、业务部门落实主责、安全团队实施内控、审计团队独立监督的“决策 - 执行 - 监督”三级联动机制。厘清权责边界，形成“业务主责、安全内控、审计监督”的制衡格局，确保制度刚性落地。

(2) 技术架构(智慧中枢，一核八翼)：构建以数据安全综合治理平台为‘智慧中枢’的顶层架构，纵向贯通组织管理、人员能力、平台工具、数据生命周期四大治理体系。依托‘一核八翼’战略，深度集成资产梳理、漏洞扫描与修复、访问控制、数据脱敏、安全审计、数据加密、运维管控、分类分级八大原子能力。通过多维联动，推动数据安全从‘分散式单点防御’向‘全域体系化智控’的跨越式升级。

(3) 运营架构(闭环智控)：构建“监测 - 响应 - 优化”动态闭环。依托全域洞察实现7×24小时实时监测与威胁预警；建立分级应急机制，确保事件分钟级响应与处置；基于审计数据定期复盘，动态迭代策略，实现从“被动合规”向“主动智控”转变。

(4) 组织架构(三级联动)：确立“决策 - 管理 - 执行”三级责任体系。决策层(数据安全委员会)统筹战略与资源；管理层(工作组)负责制度制定与跨部门协调；执行层(专职团队+业务单元)落实技术运维与源头治理。厘清“谁主管谁负责”边界，形成全员协同、权责对等的治理生态。

2.2 主要建设内容与关键技术

(1) 事前·资产可视与风险评估

部署数据资产梳理及分类分级系统，利用协议分析自动识别师生身份、科研成果等敏感数据并打标分级，结合数据库漏洞扫描，精准绘制动态数据地图，夯实策略底座。

(2)事中·场景化精准施策：

·运维场景：部署数据库防火墙，基于行为建模拦截SQL注入与越权访问，保障核心库安全。

·开发测试：实施静态脱敏，对生产数据进行不可逆仿真替换，确保“可用不可见”，杜绝测试环境泄露。

·业务共享：实施动态脱敏，对低权限用户实时掩码，高权限正常显示，平衡安全与效率。

·状态监控：实时监控数据库运行状态，及时发现异常流量与性能瓶颈。

(3)事后·溯源与统一运营：

·全流量审计与溯源：全覆盖部署数据库及运维审计，建立精细化操作日志关联机制，实现共享数据泄露的快速定责。

·平台化联防联控：搭建综合治理平台汇聚多源日志，利用自动化关联分析技术，实现安全态势可视化、威胁主动预测及多设备协同防御。

·全流程安全闭环：构建覆盖数据采集、传输、存储、处理、交换至销毁的全生命周期防护体系，确保“数据流动到哪里，安全防护就跟进到哪里”。

3 示范效应

本案例在教育行业具有极强的引领与推广价值。

一是确立治理新标准。

率先深度落地DSMM模型，构建“管理三级联动、技术立体防护”架构，探索出“基于场景的精准防护”模式，为高校提供从组织到技术的完整路径，填补行业空白。

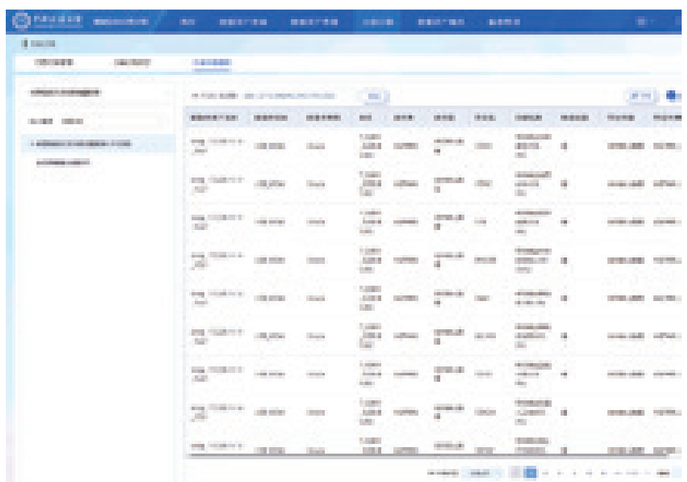
二是平衡价值与安全。

依据校级指南生成分级分类清单超12000条，通过精细化脱敏打破数据孤岛，在确保安全前提下有力支撑跨部门科研协作，释放数据潜能。

三是构建智能联防生态。

创新“平台+原子能力”模式，统一纳管MySQL、Oracle等超380个异构数据库；集成定期漏扫修复、防火墙规范运维、全量审计及动态脱敏等能力，实现从被动防御向主动感知转变。该方案不仅完全满足《数据安全法》合规要求，更形成“资产可视、风险可控、泄露可溯”的最佳实践，对推动教育行业数字化安全底座建设具有深远乘数效应。

4 附件：



华中农业大学
教育数据全生命周期安全治理与合规项目

华中农业大学

1 场景

随着教育数字化转型深入推进，华中农业大学原有数据管理模式面临制度体系不健全、数据孤岛突出、部门协同不足、安全保障薄弱、数据价值释放滞后等问题，难以满足教育数字化转型和数智校园建设新要求。学校以“数据驱动决策、服务赋能师生”为目标，立足数据全生命周期管理，创新提出“3+3”数据治理新理念——即构建“管理+技术+协同”三维工作机制，打通“安全+数据+AI”应用场景工作路径，系统推进教育数据从采集、存储、治理、共享到应用、销毁的全流程规范治理。



在管理层面，构建“1+4+1”制度体系，建立由网信办统筹，业务数据主管部门负责，信息部门技术支撑保障的跨部门协同工作机制，明确数据权责边界，形成制度闭环；

在技术层面，建设校级统一数据中台，汇聚14个部门33个业务系统共4.5亿条数据，完成13个部门4393个字段的分类分级配置，形成了“事前预防、事中管控、事后追溯”的全生命周

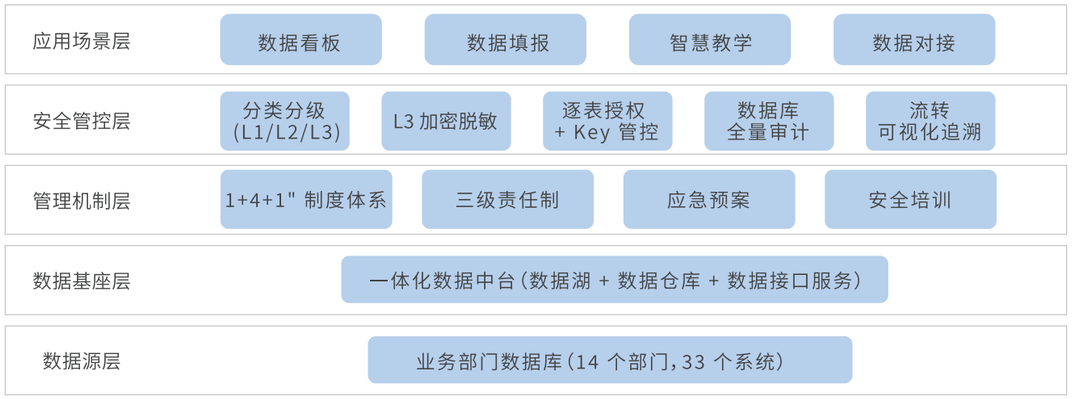
期安全防护体系，实现从“无序管理”到“精准防护”的关键突破；

在应用层面，打破数据共享壁垒，依托数据中台与AI技术赋能智慧应用场景，一年来累计提供数据接口328个、调用超1100万次，落地超20个AI应用场景，在保障数据安全可控的前提下充分释放数据价值，为高校教育数据安全治理提供了可复制、可推广的实践方案。

2 成果呈现

2.1 整体架构设计

本案例以“数据安全贯穿全生命周期”为核心理念，通过“3+3”理念落地实施，构建覆盖数据产生、采集、存储、治理、共享、使用到归档销毁的教育数据全生命周期安全治理体系。数智校园建设成效显著，数据治理能力全面提升。



2.2 制度体系日趋完善，协同机制高效运转

构建“1+4+1”制度体系：1个《教育数据管理办法》确立“谁主管谁负责、谁运营谁负责、谁使用谁负责”三级责任制；4个实施细则覆盖数据标准、质量、共享、安全管理；1个《数据分类分级指南》将个人数据细化为生物识别、身份证件、联系信息、行为记录等8大类别，制定差异化管控规则。已完成13个部门共4393个字段的分类分级：L1级（公开级）662个、L2级（内部级）2560个、L3级（敏感级）1171个。L3级敏感数据（如身份证号等）由平台强制脱敏加密，仅支持单向验证查询，前端默认脱敏显示。部门间数据共享响应时长有效缩短，实现数据管理 “有制度、有流程、有责任、有监督”，数据治理规范化、制度化水平显著提升。

2.3 技术底座坚实稳固，安全防线全面筑牢

部署专业数据库审计设备，接入全校全量数据库，实时记录所有数据访问操作行为，确保全程可追溯、可审计。逐表授权与密钥管控：实施“逐表申请、逐表授权”精细化访问控制，每张数据表须经网信办与归口部门双重审核后方发放专属访问密钥（Key），接口设置有效期，逾期自动失效，管理员可随时回收，实现数据访问权限精准授予与动态管理。传输存储安全：全校B/S系统统一采用HTTPS加密传输，L3敏感数据实现脱敏加密。监测与追溯：部署网络安全态势感知平台和多级防火墙，定期安全扫描和渗透测试，系统上线前须通过安全扫描。数据中台提供“全局数据流向地图”和“微观全程链路图”，实现从宏观到微观的全维度数据流转可视化追溯。

2.4 数据价值充分释放，智能应用落地见效

在安全可控前提下，一年来14个部门申请数据共享597次，为36个业务系统提供数据接口328个，总调用超1100万次。制订数据标准模型183个，发布403张标准代码表，数据质量自动检测推动各部门持续提升（如人力资源部评分从84.92提升至91.29）。

安全治理赋能40个数据看板、教职工一张表、本科生成长画像、智慧巡课等应用场景，在保证数据安全的前提下建成超过10个垂直领域AI应用、超20个应用场景，数据价值持续释放。

3 示范效应

3.1 行业示范价值

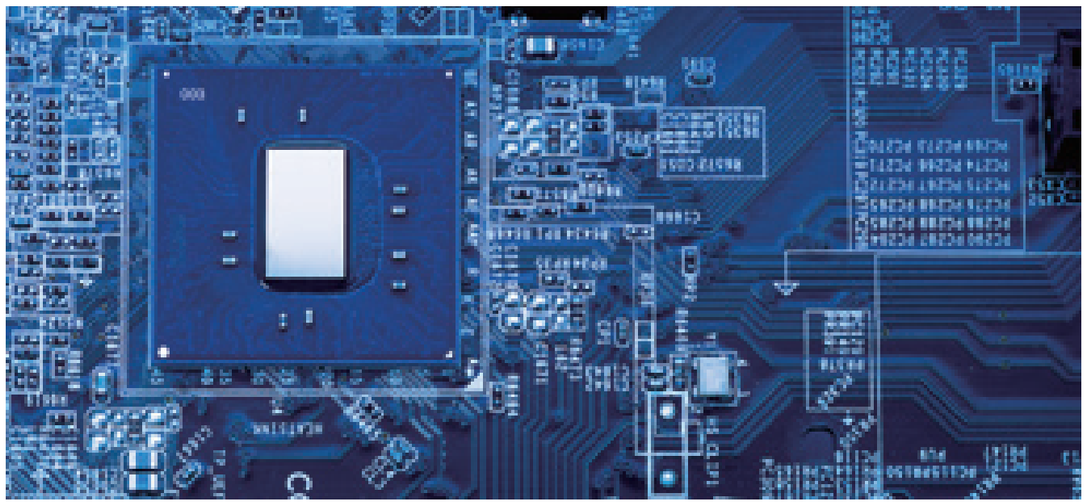
华中农业大学探索形成了“3+3”教育数据全生命周期安全治理模式，立足高校数据治理实际，破解传统治理痛点。特别是将个人数据细化为8大类别并按L1/L2/L3三级实施差异化管控的做法，为教育行业数据分类分级落地提供了可操作的参考范本。

3.2 乘数效应显著

数据安全治理与数据共享形成良性循环——安全机制的完善促进了各部门数据共享意愿显著提升，一年内14个部门597次共享申请、328个接口、1100万次调用充分证明了"以安促用、以用促治"的乘数效应。数据质量持续提升，应用场景不断涌现，数据驱动学校治理能力现代化成效显著。

3.3 案例亮点

一是全生命周期安全覆盖，从数据产生到归档销毁全链条管控；二是精准分级，差异防护，4393个字段三级分类、L3敏感数据强制加密脱敏；三是逐表授权，全量审计，通过精细管控，数据库全量审计叠加逐表密钥授权，访问可控、操作可溯；四是管理技术同步协同，“1+4+1”制度体系与技术防护深度融合，可持续、可推广。



某教育数据中心
敏感数据安全管控与防护项目

武汉通达数据科技有限公司

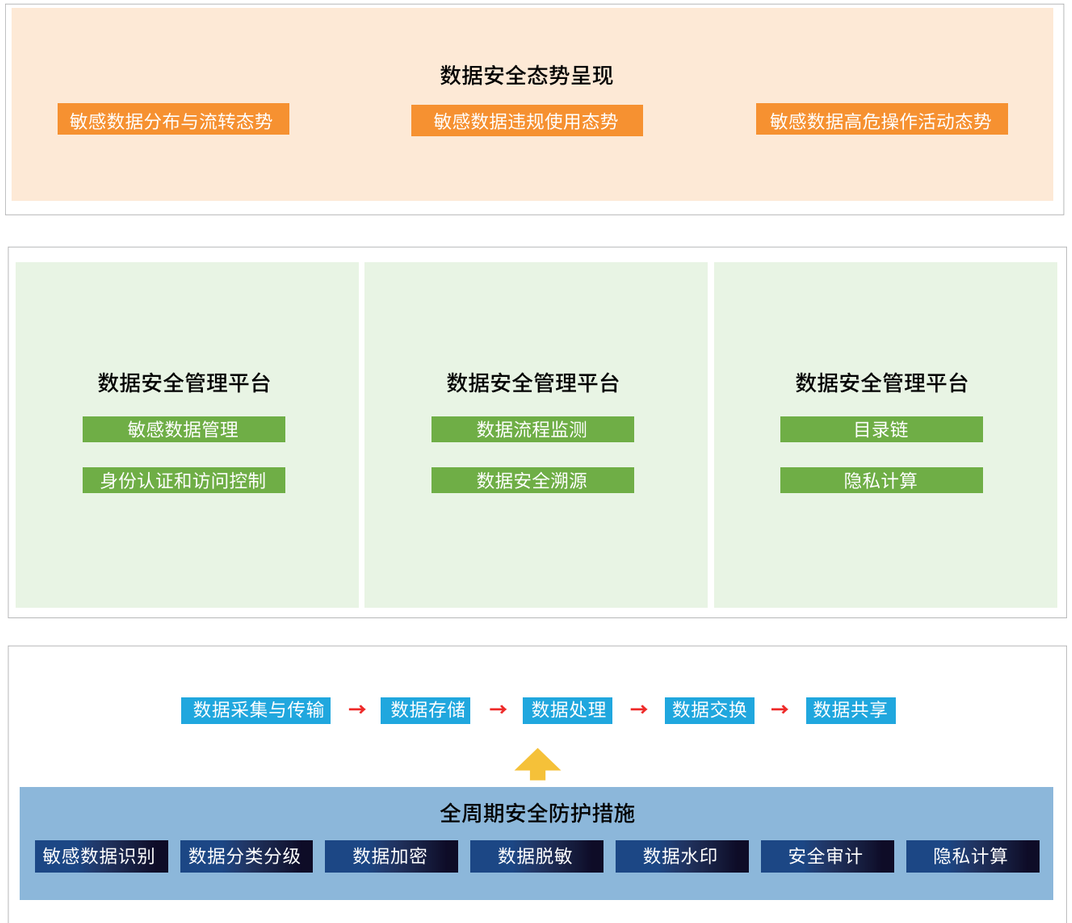


图 数据安全架构

1 场景

某教育数据中心已汇聚教师、学生、教学等数据，有效支撑各业务系统数据需求，同时也带来数据安全管理的问题，因此需要依据国家、省以及教育行业的数据要求，识别出教育数据中哪些数据是敏感数据，以及敏感数据的级别。依托数据安全软件的脱敏、加密、水印、审计等功能开展数据安全工作，实现各类敏感数据的安全管理和使用。

2 成果呈现

数据安全管理需要覆盖数据仓库中数据全生命周期，包括采集、存储、处理、交换、共享环节的数据安全管理，结合数据中心数据使用场景进行建设。通过数据安全系统建设，对数据生命周期内各使用场景进行数据安全监测，评估数据中心现有数据安全控制措施的有效性及薄弱环节，对有问题的风险场景及时进行数据安全整改，优化数据安全相关制度流程，进而持续的提升数据中心的数据安全防护能力。

本次建设包括数据分类分级、敏感数据管理、数据脱敏、数据水印、安全审计功能及数据安全服务。

数据分级分类是数据安全管理的基础，数据分级可以识别敏感数据的级别，数据分类可以按照元数据、数据来源、数据种类等维度进行分类，在数据分级分类基础上，结合用户分权、用户分类、身份鉴别、行为审计、账号管理、权限管理等措施实现数据访问的安全。

敏感数据管理实现对分级、分类后的敏感数据识别和管理，同时结合数据权限管理，对人员数据访问权限进行管控。

数据脱敏通过抹去数据中的敏感内容，同时也保持原有的数据特征、业务规则和数据关联性，保证数据服务、数据应用以及其他各类业务不会受到脱敏的影响，达成脱敏前后的数据一致性和有效性。

数据水印技术是一种基于内容的、非密码机制的计算机信息隐藏技术，将一些标识信息（即数字水印）直接嵌入数字载体当中（包括多媒体、文档、软件等）或是间接表示（修改特定区域的结构），且不影响原载体的使用价值，也不容易被探知和再次修改，但可以被生产方识别和辨认。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。

数据安全审计技术从多个维度抽取数据，并进行关联、分析，形成风险判断和违规告警，并对风险趋势进行预测，发布数据安全风险预警。

数据安全服务是编制符合实际的分类分级细则，按照分类分级细则对数据中心数据进行数据分级分类并进行敏感数据管理，通过数据脱敏对数据进行脱敏或加密，对人员进行数据访问权限设置，并对共享数据注入水印，以便后续追踪数据流转。最后通过审计规则配置、日常巡检保障数据安全。

3 示范效应

模式标准化：针对数据分类分级形成清晰的操作流程、制度文档，便于跨组织复用。

降低试错成本：通过发布《字段级别判定表》、《教育数据分级申报表》、《教育数据安全风险评估指引》等文件，减少探索周期。

安全指标提升：实施敏感数据分级后，数据泄露风险下降、合规审计通过率提高。

动态更新机制：数据分类分级的动态更新机制，确保制度不僵化。

教育行业考试报名系统数据安全风险评估与整改项目

武汉安域信息安全技术有限公司

1 场景

在教育数字化转型持续深化的背景下，高考、成考等各类考试报名系统作为教育领域重要业务载体，承载大量考生敏感信息及考试组织相关数据，具有数据体量大、敏感度高、覆盖范围广、安全责任突出的特征，其数据安全直接关系教育领域公信力与社会公共利益。本案例以数据安全优先为核心原则，将数据安全管控要求贯穿数据全生命周期，依据GB/T43697-2024、GB/T45577-2025及《教育数据分类分级指南》征求意见稿，结合行业最佳实践，开展数据分类分级与风险评估工作，着力解决系统数据安全防护体系不完善、风险研判不精准等问题，保障数据安全合规，为教育行业数据安全治理工作提供可复制、可推广的标准化实践范式。

2 成果呈现

本案例遵循国家数据安全治理相关标准及教育行业最佳实践，采用“数据资产梳理→分类分级→风险评估→治理优化”四层递进式逻辑架构，各层级协同联动、闭环衔接，全面覆盖数据全生命周期安全管控，保障治理工作规范有序。



2.1 逻辑架构设计

数据资产梳理通过系统扫描、专项访谈、文件审核等手段，摸清系统数据分布、类型、存储及访问权限，建立标准化资产清单与调研记录，实现数据全流程可管可查可控；

分类分级依据国标及行业指南制定专属标准，将数据划分为核心、重要、一般三级，完成标识审核上报，形成重要数据目录并建立动态更新机制；风险评估参照国标框架，梳理业务场景、识别全生命周期风险，采用定性方法，形成风险清单及专业评估报告；

治理优化依据评估结果制定防控方案，完善制度、部署防护措施，建立闭环管控机制并开展专项培训，实现风险动态防控。

2.2 主要建设内容

梳理数据资产，明确数据所有者、存储位置等核心信息，完成资产测绘并形成台账及清单；制定分类分级规范，完成全量数据标识审核，形成相关规范及清单；构建风险评估模型，识别系统风险，形成风险等级清单、分析报告及处置建议；完善数据安全管理制度，明确访问管控、加密等核心要求，健全应急预案；部署数据加密、细粒度访问控制等技术防护措施，构建全方位防护体系。

2.3 关键技术支撑

采用表单工具结合人工审核模式，遵循分类分级国标完成数据分类分级，保障合规准确；参照数据安全风险评估国标中的框架，结合行业特点构建风险评估模型，提升评估精准度；采用国家密码标准加密数据，结合RBAC模型实现细粒度访问控制，防范各类安全风险。





某高校量子科技创新及校园量子加密通信网搭建项目

中国电信股份有限公司武汉分公司

1 场景

在教育数字化转型持续深化的背景下，高考、成考等各类考试报名系统作为教育领域重要业务载体，承载大量考生敏感信息及考试组织相关数据，具有数据体量大、敏感度高、覆盖范围广、安全责任突出的特征，其数据安全直接关系教育领域公信力与社会公共利益。本案例以数据安全优先为核心原则，将数据安全管控要求贯穿数据全生命周期，依据GB/T43697-2024、GB/T45577-2025及《教育数据分类分级指南》征求意见稿，结合行业最佳实践，开展数据分类分级与风险评估工作，着力解决系统数据安全防护体系不完善、风险研判不精准等问题，保障数据安全合规，为教育行业数据安全治理工作提供可复制、可推广的标准化实践范式。

2 成果呈现

2.1 逻辑架构设计

以“产学研用”深度融合为核心导向，共建“武汉量子科技联合创新中心”。创新中心采用“一中心两基地”模式，形成“三方协同、双地联动”的布局。整体构建“联合创新-学科建设-人才培养-场景应用”的闭环逻辑架构，同步配套完善的架构支撑体系（逻辑架构图聚焦三方协同流程、职责分工及联动机制，技术架构图涵盖量子计算、量子通信等核心技术模块、设备部署及数据流转路径），为项目落地提供坚实支撑。

2.2 主要建设内容：

1. 共建联合创新中心，搭建三方协同创新平台，秉持“优势互补、资源共享、协同创新、共赢发展”原则，构建量子科技发展生态；

2. 推进量子特色学科建设，联合开发量子专业教学课件、共建量子信息实验室及教研平台，完善学科教学资源；

3. 打造专业化实验方案与生产实习方案，依托电信资源构建“理论学习—仿真推演—真机实操”全流程实训体系，配套相关指导手册与案例库；

4. 建设校园量子加密通信网，完成量子安全服务私有化平台及4个用户站部署，保障校园数据安全。量子校园项目组网示意图如下图所示。

2.3 解决问题

3 示范效应

案例参照国家数据安全标准及行业最佳实践，融合国标及教育行业相关规范，形成“分类分级+风险评估”一体化实践范式，其示范效应与乘数效应具体体现在以下方面：

行业引领：为教育行政主管部门、各级院校及相关教育机构开展数据安全风险评估工作提供标准化操作指引，契合教育行业数据安全治理需求，推动教育行业数据安全治理体系规范化、标准化建设。

技术推广：案例所采用的分类分级方法、风险评估模型及技术防护措施，贴合国家数据安全标准及行业最佳实践，可广泛应用于教育领域各类业务系统，全面提升教育行业整体数据安全防护水平。

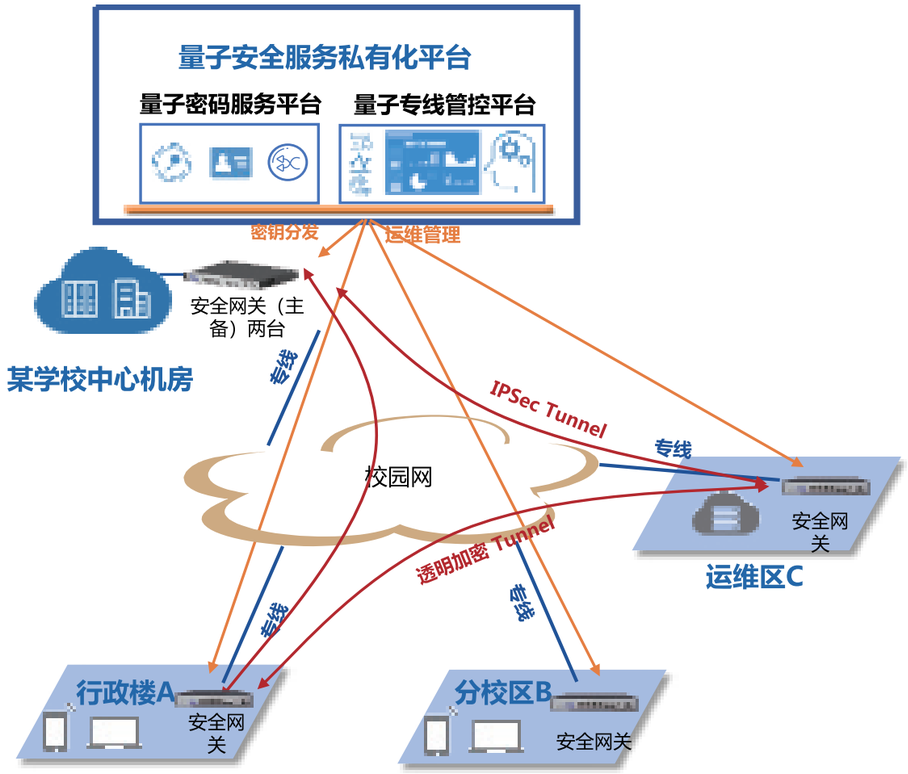
合规保障：助力各类教育机构精准落实国家数据安全相关法律法规及标准要求，有效降低数据安全合规风险，增强社会公众对教育数据安全的信任度，为监管检查提供规范的合规依据。

乘数效应：通过案例推广应用，可带动教育行业数据安全产业链协同发展，推广标准化服务模式，促进数据安全产品与服务创新升级，构建“以点带面、全域提升”的教育行业数据安全生态体系。

有效破解了量子信息科学专业（2023年新增本科专业）核心实验课程无法开展、专业实验室缺失的教学痛点，满足在校生逐年增长的实验教学需求；弥补学科硬件设施不足的短板，助力学校“双一流”建设及省级重点实验室申报，为学科评估提供硬件保障；衔接高校人才培养与企业实际需求，通过双导师制、实践实训等模式，解决量子领域创新型、复合型人才供给不足的问题；构建高等级校园量子安全防护体系，抵御量子计算攻击，杜绝数据窃取、篡改风险，保障校园核心业务数据传输安全。

2.4 关键技术

依托中国电信“天衍”量子计算云平台及超导量子计算机资源，为量子计算研究与教学提供算力支撑；融合量子安全加密技术与SM2/SM3/SM4国密算法，提升加密通信安全性与兼容性；采用量子安全加密网关旁路部署技术，不改变原有校园网络架构，将加解密时延控制在≤200us，满足城域网传输指标；构建“理论-仿真-实操”一体化实训技术体系，有效支撑量子纠缠、量子密钥分发、量子精密测量等核心实验开展。核心架构图如下图所示。



项目组网示意图



核心架构图

目前项目四大攻坚目标均已圆满完成，成功建成中部地区量子科技领域技术创新高地、产业应用枢纽和高端人才培养摇篮，有效推动高校量子学科跨越式发展，助力区域量子科技产业高质量发展。

3 示范效应

本案例的亮点是采用“政企校”协同模式，以“一中心两基地”为载体，实现量子技术、学科建设与高校场景的深度融合。其示范效应显著，为国内量子科技与教育融合提供可复制范本，引领高校量子学科建设与企业技术落地协同发展。乘数效应方面，可推动量子教学科研成果快速转化，培育专业人才，带动量子校园网、量子教学设备等相关产业发展，助力区域量子生态完善，既完善高校量子教学实验条件，又推动量子技术产业化落地，实现科教与产业双向赋能。

某财大智慧校园数据安全综合治理与防护项目

杭州安恒信息技术股份有限公司

1 场景

中南财经政法大学是教育部直属“双一流”“211 工程”重点建设高校，教育部、财政部与湖北省三方共建高校。校园数智化转型深入，海量师生敏感信息、教研核心数据全链路流转，安全合规需求迫切。学校已搭建基础安全防护框架，但尚未形成管理、技术、运营一体化的数据安全防护体系，体系短板凸显，数据中台建设为体系升级带来关键契机。

本案例锚定合规防护核心，创新应用数据分类分级智能体工具，高效梳理多核心业务系统数据，落地全局分类分级管控、全流程数据监测审计。项目破解了合规短板、风险难发现等痛点，筑牢校园数据安全防线，打造高校场景可复制标杆范式，为教育行业数字化转型提供示范引领。

2 成果呈现

本案例整体逻辑架构设计以“合规为引领、技术为支撑、运营为保障”，构建管理体系、技术能力、运营体系三位一体、协同联动的闭环架构，贯穿数据全生命周期，核心是通过三大维度有机融合，搭建体系化的高校数据安全保障体系，实现“制度健全、技术完备、运营高效”的建设目标，适配中南财经政法大学数据安全管理的实际需求。

（一）数据安全管理体系上，聚焦合规能力提升、管理机制完善和监管运营基础夯实，搭建数据安全组织架构、明确职责分工，建立覆盖个人信息安全、应急处置、运维管理等的制度流程，构建跨部门协作体系，实现制度与技术管控联动；

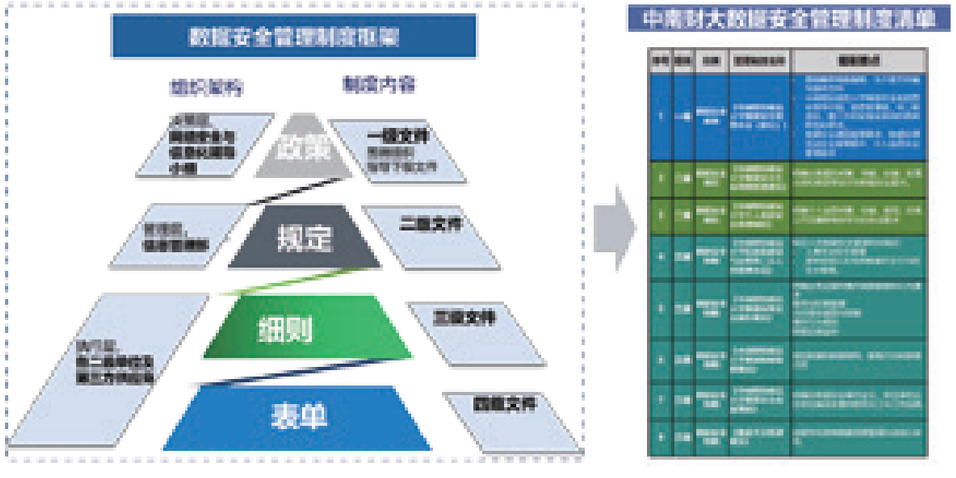
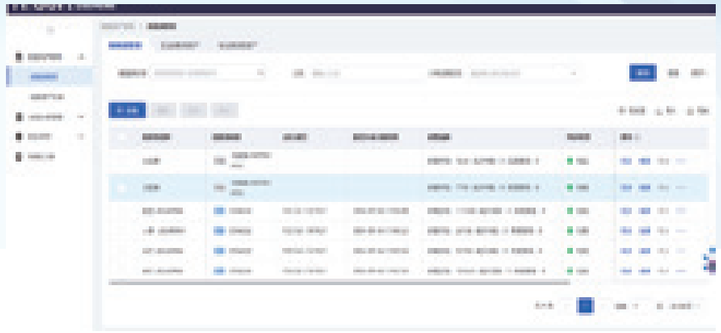


图 数据安全管理制度

（二）数据安全技术上，结合人工智能技术的创新应用，通过数据分类分级智能体，高效完成全校人事、学工等多系统数十万字段数据并建立全局管控台账，支撑分类分级管控。



分类分级结果呈现

通过数据安全技术工具实施记录分析数据库操作及API调用，构建敏感数据流向监测、异常告警及安全事件追溯机制；



API调用审计风险呈现

数据安全运营上，开展定期安全评估与常态化运维闭环，搭建了基于数据安全管控平台的实时敏感数据集中管理与动态监控，同时建立分层分阶段培训规划，提升相关人员安全素养与处置能力。

项目以AI分类分级、数据资产可视化、数据库及API全局审计技术、数据安全态势感知技术，为数据安全管控、异常监测和事件追溯提供核心能力支撑，助力实现数据安全全流程、全方位防护。

3. 示范效应

创新融合AI+数据分类分级技术，依据教育部指南打造校本化分类分级框架，精准管控 16541个3级敏感数据字段高危操作；构建“制度 + 技术”双重保障，配套全流程审计、智能监测告警与事件追溯响应机制，实现合规管控、精准防护、快速处置全闭环。

该案例破解了高校多系统敏感数据管控难、合规适配难等行业痛点，为全国各类高校、教育机构提供了可落地、可复制的实践范式。其精细化主动管控的建设思路，可为党政机关、事业单位提供参考借鉴，推动教育及相关领域数据安全治理从被动防御向主动管控转型，形成跨领域行业乘数效应，助力全行业提升数据安全合规与精细化治理水平。

湖北国土职院智慧校园数据共享与安全防护项目

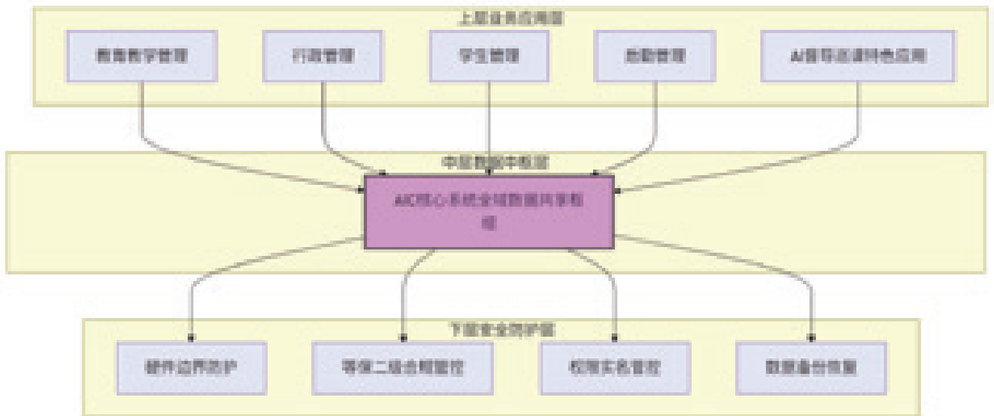
湖北国土资源职业技术学院

1 场景

我校自2017年聚焦数据应用导向，以AIC系统为核心打通全业务系统，覆盖教育教学、行政管理、学生管理、后勤管理全场景，还落地AI督导巡课特色应用，实现全域数据共享、打破信息孤岛，为智慧校园数字化转型筑牢基础。伴随数据深度流通与AI场景落地，数据泄露、网络入侵、权限越界、系统合规风险等安全隐患凸显，成为数字化推进核心挑战。我校立足现有业务融合基础，聚焦数据安全防护、合规管控、应急保障三大需求，构建软硬件协同、全流程闭环的安全防护体系，破解数据共享与安全保障矛盾，有效抵御内外网攻击，保障系统合规运行，实现数据赋能与安全防护同步推进，做法获省教育厅、省公安厅认可，相关经验以《数字筑基职校园网络安全的创新实践》登载于《数字化时代的荆楚教育变革：湖北教育数字化典型案例》，具有较好的实践借鉴和推广意义。

2 成果呈现

整体逻辑架构：采用“数据赋能+安全兜底”双向架构，以AIC核心系统为数据枢纽，前端打通全业务系统实现数据共享，后端搭建“硬件防护+合规管控+应急保障”三维安全防线，形成“采集-共享-应用-防护-备份”全生命周期数据安全闭环，兼顾数据流通效率与安全管控力度。配套逻辑架构图清晰拆解三层联动关系，如下：



逻辑架构图

整套架构实现业务应用、数据枢纽、安全防护无缝衔接，既保障AI督导巡课等场景数据高效调用，又筑牢全流程安全屏障。

主要建设内容：一是硬件防护升级，部署边界防火墙、WEB防火墙、态势感知研判与预警系统，筑牢网络边界防线，精准拦截外来入侵与校内横向信任攻击；二是合规管控落地，全面落实信息安全等级二级保护要求，严把业务系统上线合规关口，实现全系统合规运行；三是权限与接入管控，推行端口最小化、权限最小化原则，实行网络用户实名接入，全程留痕、有据可查；四是应急机制完善，搭建数据备份与恢复体系，防范数据丢失风险。

关键技术与解决问题：依托态势感知、边界防护、分级授权、实名准入等技术，解决数据共享后的网络入侵、数据泄露、权限混乱、系统不合规、数据丢失等痛点，实现安全防护无死角、管控无漏洞。配套技术架构图拆解四大技术模块，如下：



配套技术架构图

技术架构聚焦实战防护，针对性破解数据共享与AI应用带来的安全风险，全程可监控、可追溯、可应急。

3 示范效应

本案例打破“数据共享与安全防护难兼顾”的行业痛点，构建了“先赋能、再防护、全合规”的校园数据安全建设模式，具备鲜明示范价值。亮点突出：一是软硬件协同防护，兼顾数据流通性与安全性；二是全流程合规管控，贴合教育行业信息安全标准；三是精细化权限管理，实现风险可防可控可追溯。案例获登《数字化时代的荆楚教育变革：湖北教育数字化典型案例》，形成可复制、可推广的校园数据安全建设范式，为各级各类学校数字化转型中的数据安全保障提供参考样本，助力行业筑牢数字安全屏障，推动智慧校园高质量发展。

湖北大学云网安运管平台建设项目

湖北大学

1 场景

2024年3月，湖北大学前瞻布局，正式成立大数据中心，全面启动智慧校园2.0建设，致力于通过“五个一”工程打造统一、高效、安全的数字新生态。作为此次建设的压轴环节与关键基石，“云网安运管平台”项目的成功选型至关重要。经过多方严格调研与论证，湖北大学最终携手武汉吧哒科技股份有限公司，以其自主研发的信服易云运维一体化管理软件作为核心引擎，共同绘制智慧校园的安全蓝图。

心集运维、流程、安全、数据于一体的综合管控运管体系，是数据安全的重要支撑，深度融合资源管理、监控、机房可视、ITSM、安全态势五大模块，通过CMDB与运维场景深度联动，帮助团队实现“资产-监控-处置-优化”闭环运维，大幅提升运维效率，将IT问题对业务的影响降至最低。

满足等保、数据安全法、云边协同与集约化建设需求，对异构设备平台集成管理，构建统一资产台账及运维管控，以统一化、可视化、平台化能力放大运维、安全、效率、成本、合规、数据等综合价值，支撑业务稳定与数据安全双提升。

2 成果呈现

云网安运管平台是一款以CMDB（配置管理数据库）为核

2.1 整体逻辑架构设计



逻辑架构图

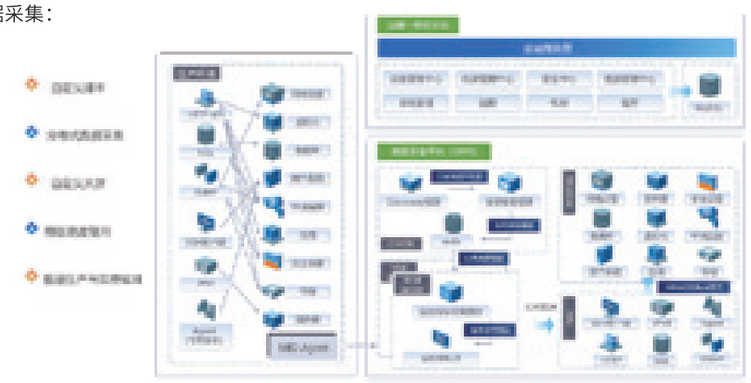
2.2 整体技术架构设计



整体技术架构图

2.3 平台关键技术

多源异构数据采集：



数据采集技术原理图

3 示范效应

云网安运管平台在教育行业成功应用构建融合“统一运维监控+集中配置管理+运维流程线上化+巡检自动化+安全态势可视化”的一体化平台。将运维“对象”“状态”“行为”“安全”四大要素进行数字化重塑与平台化承载，实现技术与管理深度融合，为“云网安”统一运营管理奠定基础。

以“运维数据”为核心，通过统一模型构建，梳理基础设施、业务应用等分层对象模型，形成精准业务拓扑、网络拓扑。引入运维知识图谱技术，以CMDB为基座，通过物理连接、部署关系等多维度展现配置项复杂关系，图形化呈现关联，为故障分析提供可解释依据，实现流程规范化与AI智能作业编排动态调度。

在云网安运管平台的落地，为湖北大学带来了超越预期的综合价值变被动“救火”为主动“防火”，运维效率显著提升，IT团队得以从繁琐重复的工作中解放，专注于战略创新。构筑了“监测-预警-处置-溯源”的全链路安全防线，全面提升了学校应对新型网络威胁的能力，让智慧校园运行更稳健。强大的平台能力确保了全校师生在任何时间、任何地点都能享受到流畅、稳定、安全的数字化服务，极大提升了教学科研的满意度和幸福感。

开放式云化校园网络

星融元

1 场景

河北某大学（BHLG）建筑面积131,700平方米，日常有13,000多名教职工和学生，30,000多台设备终端。随着教学和科研活动的不断发展，学校面临着日益增长的网络流量和设备接入需求。因此，迫切需要升级现有网络基础设施，以确保其能够满足未来的需求。

1.低延迟、高性能的网络设计，以支持大量设备接入

2.校园无线网的无缝漫游和高效管理

3.一站式的网络控制平台，统一纳管监控整网有线无线设备，以帮助运维人员简化操作任务

4.统一的流量采集和监控能力，同后端数据安全产品联动，确保关键数据安全

2 成果呈现

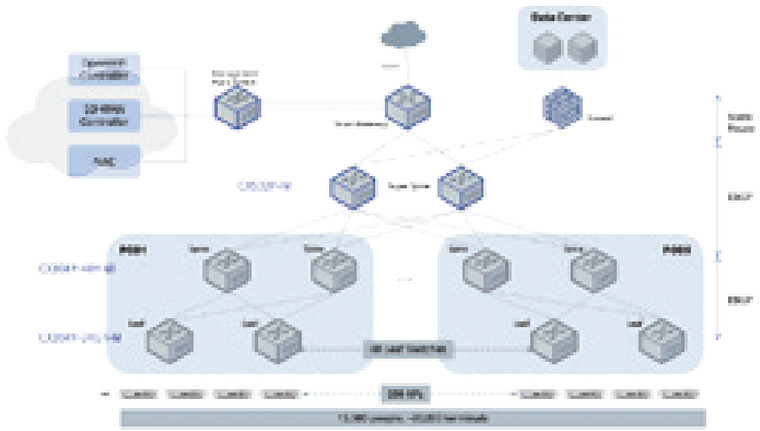
星融元提供的网络解决方案将云数据中心网络的理念与架构有机引入园区，将网络划分为五个Pod，通过两台CX532P-M作为Super Spine交换机实现互连。这种设计提高了网络的可扩展性、容错性和性能。

IP路由规划的优化：采用了全三层的网络架构，彻底杜绝广播风暴，并利用了IP路由聚合技术，显著优化了MAC地址和路由表的管理，从而轻松满足未来的扩展需求，减少硬件升级频率。

Wi-Fi漫游延迟改善：采用创新的分布式网关（无AC）设计，将Wi-Fi切换延迟降低至约10毫秒，同时拥有超大漫游域。

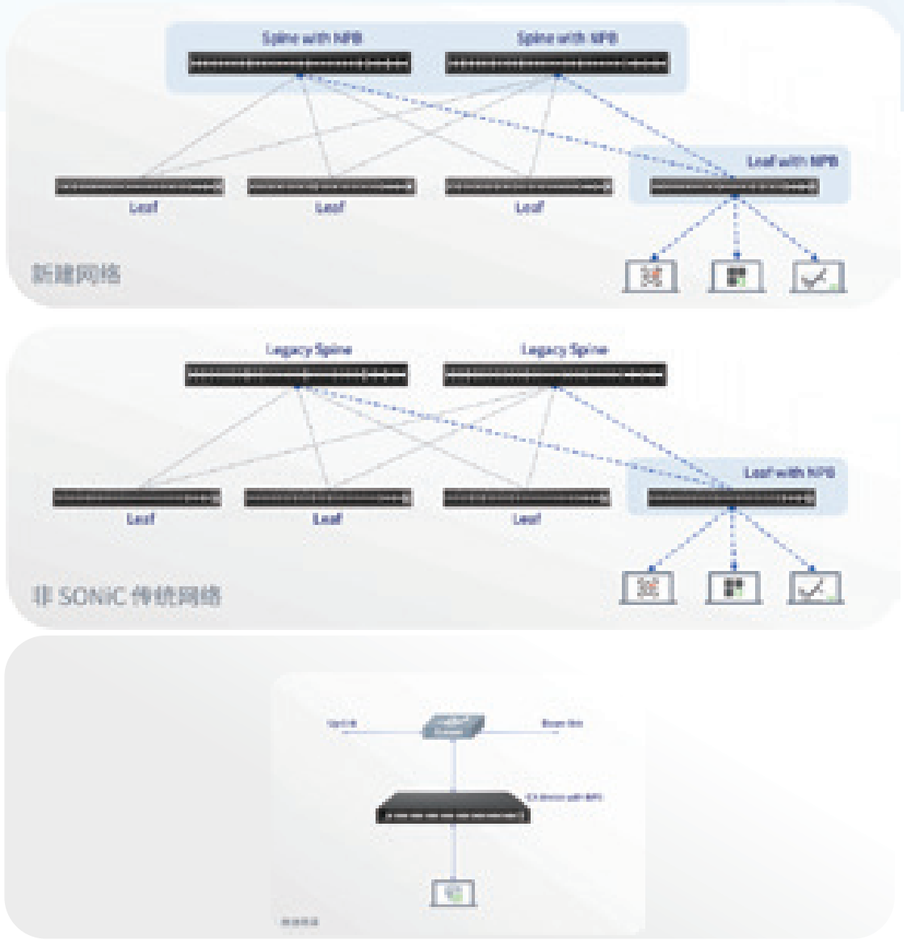
网络出口架构升级：BorderLeaf交换机+智能网关平台组合，提供网络流量的安全路由和转发性能，支持百万级路由表、负载均衡和流量管理功能。

一站式运维管理：基于星融元园区网络控制器（ACC），统一管理637个AP和数百台园区交换机，终端设备可管可查，便于问题溯源。



流量采集与分析：该方案充分利用SONiC交换机容器化开放架构的强大功能，将数据包代理功能无缝集成到单个容器中，由高性能Spine交换机执行旁路的流量镜像和过滤功能，而无需额外的分流器/TAP交换机。

此方案同样适用于串接部署场景，运行NPB容器的交换机可主动进行流量调度，可按需引导被监管流量进入安全分析设备完成检测，从而支持实时阻断风险流量。



3 示范效应

本案例作为把云数据中心内部广泛引用的Spine-leaf架构引入到大规模园区网的样本点案例，突显了新一代云化园区为大型教育机构构建高性能网络解决方案的架构级优势，充分展现了我们的技术专长和行业经验，使客户校园网络在性能、稳定性、可扩展性和维护管理方面均实现了显著提升。

教育行业数据安全典型案例

湖北某省属“双一流”高校

1 场景

湖北某省属“双一流”高校，位于湖北省武汉市，是一所综合性大学实行省市共建、以市为主的办学体制，入选湖北省“双一流”建设，“国内一流学科建设高校”。

结合数据安全法和等级保护政策要求，通过数据安全体系的建设，加强数据安全管控能力，提升数据安全管控视野，切实履行数据安全工作落实的监督职责，对数据资产实现全面识别和监控、对系统数据安全风险态势进行实时动态评估、为合规性评测提供检查和整改的流程通道，确保学校大数据、一卡通、网站等业务系统全程可知、可控、可管、可察，变静态为动态，变被动为主动，为数据挖掘、科研分析和决策支持提供有力支持，为学校数字化转型建设提供严密数据安全保障。

2 成果呈现

2.1 学校数据安全现状

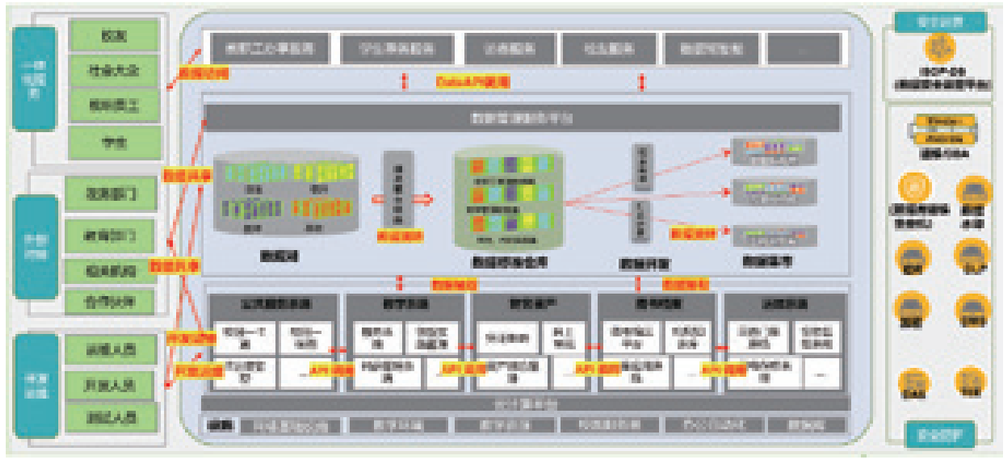
数据跨学院、跨部门流转，涉及不同院系、部门，没有统一团队、专业人员牵头，无法形成统一数据安全防护体系；

数据流通性强，涉及多个院系、部门的人员，数据安全事件发生后，难以有效溯源，缺乏认责依据，无法认责造成无所顾忌；

校园内部敏感信息泄露、以及敏感信息数据使用情况、违规访问和泄漏分析的日志记录，缺乏统一分析去溯源；

对于运维人员、开发测试人员使用数据流程和方法缺乏监控；

数据库没有厂家运维，版本过低不能升级新版本，数据库容易被攻击；缺乏数据识别、审计能力；



2.2 解决思路

1、通过数据发现与评估系统(IDR)，结合人工服务，对数据进行分级分类，从而进行策略定制；

2、部署数据安全智能分析平台(ISOP-DS)，采集敏感信息数据使用情况、违规访问和泄漏分析的日志记录等数据，同时分级分类进行统一呈现；

3、部署数据防泄漏系统(DLS)，通过分析网络流量识别敏感数据（包括图片中的文字）并进行阻断；

4、部署数据脱敏系统(DMS)，对运维人员、开发测试人员访问数据的状态和变化进行记录、保护和审计；

5、部署数据库审计与风险控制系统(DAS)，实时记录数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行实时告警；

6、部署数据库防护系统对用户、操作和对象进行访问控制的限定；

7、通过数据安全运营服务，定期监测和分析数据防泄漏、数据库审计等检测防护设备的告警和日志，及时发现数据安全威胁事件，以及应急响应与处置；

交付物

◉《数据资产清单》

◉《数据资产核查报告》

◉《数据安全威胁事件分析报告》

◉《数据安全威胁事件记录表》

◉《分析平台及探针规则优化清单》

◉《威胁事件回溯与处置报告》（按实际发生提供）

◉《设备及平台巡检报告》

◉《设备及平台维护记录表》

◉《设备基础信息收集表》

◉《设备及平台故障报告》（按实际发生提供）

◉《设备策略调整报告》

◉《应急响应处置记录表》（按实际发生提供）

◉《应急响应报告》（按实际发生提供）

3 示范效应

案例特点

聚焦高校数据汇聚、共享、开放核心场景，精准覆盖学籍、身份等敏感数据防护需求；以《数据安全法》《等保 2.0》等法规为合规底座，全流程对标政策要求；采用“技术+运营+流程”三位一体模式，明确校方与运营团队职责；按建设、运营、改进三阶段落地，低风险易推进；覆盖数据全生命周期防护，适配高校运维力量薄弱现状。

案例亮点

以平台实现数据资产自动扫描、月度稽查与基线更新，建成校园数据资产“一本账”；联动DLP、数据库审计等设备，形成威胁监测 — 研判 — 处置 — 回溯闭环；统一运维安全设备，保障巡检、升级、策略调优常态化；建立轻量化应急响应机制，快速控损溯源；输出标准化报告与月报，便于管理与汇报；形成可直接复制推广的高校数据安全运营模板，为教育行业提供落地示范。

基于信创架构的数据安全与云化升级项目

某省属重点高等院校

1 场景

1.数据安全防护机制薄弱：关键的科研成果数据和师生个人敏感信息缺乏系统级的加密与防泄露机制，数据在网络传输和长期存储过程中存在被窃取或篡改的高风险。

2.底层架构缺乏自主可控：为响应国家教育信息化与信创政策的整体规划，学校亟需采用国产化软硬件体系，完成对原有VMware架构的无缝替代升级。

3.网络边界安全隔离不足：不同院系和职能部门的业务系统处于混合部署状态，缺乏有效的安全隔离手段，一旦某处单点被恶意突破，极易引发横向的安全威胁蔓延。



2 成果呈现

为彻底解决上述痛点，该校选用了云宏CNware WinSphere服务器虚拟化软件与CNware WinStack虚拟化云平台，结合数十台国产鲲鹏服务器，构建了全面自主可控、原生具备高安全能力的新一代虚拟化资源池。

1.无感平滑的 VMware 国产化替代：项目组借助云宏提供的跨平台直迁与云迁移工具（V2V），将原有VMware平台上的数百台核心虚拟机（包含操作系统与业务数据）平滑无损地迁移至云宏 WinSphere 平台，全程通过增量同步保障数据一致性，大幅缩短了业务的停机切换窗口，实现了底层架构的国产化平稳过渡。

2.原生商用密码与数据传输安全：平台在安全设计上深度融合了国家商用密码算法，对系统内的敏感信息和关键科研数据进行强有力的加解密防护，完全符合教育行业的信息化密评规范要求 。针对虚拟机跨节点迁移、平台运维访问等过程，系统底层嵌入了SSL隧道加密保护机制，有效防止了科研与教务数据在网络传输链路中被恶意窃取 。

3.全方位的虚拟网络边界隔离与访问控制：基于VPC（虚拟私有云）网络技术，学校为财务处、教务处、重点科研实验室等不同业务部门划分了完全独立的虚拟数据中心。通过部署虚拟机安全组、分布式防火墙以及微分段技术，实现了东西向院系网络的安全隔离与南北向外部业务的安全防护。同时，在系统虚拟网卡层面全面启用了IP/MAC地址绑定功能，从根源上防止了虚拟机用户擅自修改IP或MAC地址所带来的仿冒攻击和网络冲突隐患。

4.数据全生命周期保护与安全销毁：针对校园核心数据库，平台采用了底层无代理备份机制，无需在虚拟机操作系统内安装任何额外的插件，直接通过Hypervisor层进行快照备份与恢复，全程不影响教学系统的正常运行。在虚拟机或虚拟磁盘面临报废退役时，平台提供虚拟磁盘数据安全擦除功能，对底层数据块进行高强度的置零擦除，确保废弃的科研实验数据无法从物理硬件层面被恢复，彻底杜绝数据泄密隐患。此外，结合云盘系统具备的精细权限管控、文件操作审计日志与文件水印功能，为日常教学资料的流转提供了统一的安全管理闭环。

3 示范效应

1.全面筑牢校园数据安全防线：从虚拟化内核、网络微隔离、加密传输到存储数据擦除，项目为学校实现了端到端的全方位安全加固，建立起符合国家等保要求的教育信息化公共安全保障环境，师生隐私与核心科研数据得到了最高级别的保护。

2.实现信创落地与自主可控演进：方案全面兼容适配了国产服务器芯片与主流操作系统，成功替代了国外VMware架构，消除了底层技术的“卡脖子”风险，为学校的数字教学提供了稳定、安全、可控的承载基座。

3.大幅提升资源利用与运维效率：通过统一的虚拟化云平台实现了全校计算与存储资源的池化集约管理，有效降低了数字数据中心的总体拥有成本（TCO），并能够弹性、敏捷地响应各类新设专业的教学扩容需求。

高校基于“态势感知+数据中心防火墙”的内网横向攻击隔离与数据安全治理项目

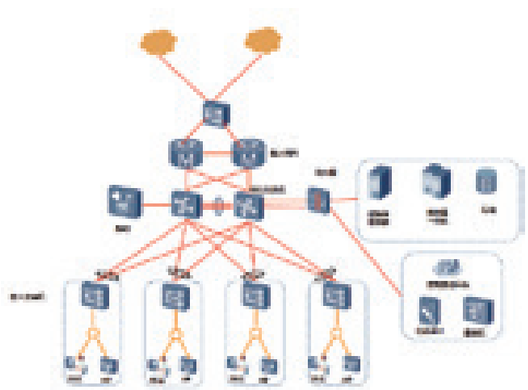
湖北大学知行学院

1 场景

在教育数字化战略加速推进的背景下，高校存储的教务数据、师生个人信息、科研数据等核心资产价值日益凸显，同时成为勒索病毒、APT攻击和数据泄露的重灾区。学校前期已按等保2.0要求部署了态势感知与数据中心防火墙，具备流量探针、日志采集器、分析引擎和边界隔离的能力。在实际运行中发现，外部攻击固然危险，但内网横向移动攻击的危害更为隐蔽和致命——一旦某台终端或服务器被突破，攻击者会迅速在内网横向扩散，窃取数据库、篡改业务系统。传统边界防火墙仅关注南北向流量，对内网东西向流量缺乏有效隔离。学校数据中心防火墙部署于核心交换机与各业务区域之间，具备精细化的区域隔离和东西向流量访问控制能力。安全团队面临三大痛点：一是告警过载，态势感知平台每日产生数百条告警，大量误报和低危告警充斥其中，真实威胁难以快速甄别；二是响应断层，发现攻击后需人工研判和手动处置，应急响应依赖个人经验，平均处置时长超过1小时；三是溯源困难，虽然有集中日志存储，但缺乏智能化的关联分析能力，完整还原一次数据泄露事件需数小时甚至数天。在此背景下，学校充分挖掘态势感知平台自身能力，通过智能告警分诊、和多维度溯源分析能力，构建“监测—分析—响应—溯源”一体化数据安全治理体系。

2 成果呈现

2.1 逻辑架构设计



2.2 数据中心防火墙结合态势感知平台隔离内网横向攻击的优势与特色

区域隔离，阻断横向扩散路径：传统出口防火墙只在出口防护边界，一旦攻击者突破边界进入内网，即可畅通无阻地各业务区之间横向移动。学校数据中心防火墙在核心交换机与各业务区域之间实施区域间默认拒绝策略，任何跨区域访问都需明确授权。即使某台学生终端被植入木马，攻击者也无法直接访问教务服务器或数据库，横向攻击链被有效切断。这是学校数据中心防火墙最核心的特色优势。

东西向流量可视与精细化控制：防火墙启用内网东西向流量的深度检测，能够识别RDP暴力破解、SMB远程溢出、数据库非法查询等横向攻击特征。同时支持基于用户、应用、时间、VLAN的精细化策略，极大缩小了攻击暴露面。

快速隔离受灾主机：当态势感知平台检测到某IP正在进行内网扫描或爆破时，安全管理员可登录防火墙一键执行“隔离”动作——将该IP加入黑名单，该IP将无法访问任何核心业务区域，有效遏制攻击者横向扩大战果。

2.3 主要建设内容与解决问题

解决“横向攻击发现后无法快速隔离”问题：通过态势感知平台的横向攻击检测能力与数据中心防火墙的人工联动，极大地缩短了响应时间。

解决“告警过载”问题：充分利用态势感知平台的智能告警分诊技术，自动过滤无效告警、精准识别高危威胁。运维人员不再逐条查看每日数百条告警，仅聚焦平台筛选后的高价值威胁告警，真实威胁识别效率大幅提升，有效破解了“告警疲劳”难题。

解决“响应断层”问题：基于预置的标准化处置流程，根据实时场景自适应决策响应，快速生成应急响应预案，实现告警研判后的自动化处置。对勒索软件、挖矿木马等常见威胁实现自动化封堵，将平均响应时间从小时级缩短至分钟级。

解决“溯源困难”问题：依托平台的大数据检索和关联分析能力，利用内置的专家经验模型，对攻击事件进行完整的攻击故事线还原，从告警时间、源IP、目标资产、攻击手法、受影响数据等多维度进行关联溯源，支撑数据安全事件的完整审计追溯。

2.4 建设成效

项目实施后，日均告警量从数百条降至数十条，无效告警消减80%以上，真实威胁识别准确率提升至95%以上。学校也成功阻断多起内网横向攻击事件。典型案例：某学生宿舍终端因下载带毒软件被控，攻击者试图通过SMB爆破横向入侵教务服务器，态势感知平台检测到异常扫描后告警，安全管理员在10分钟内登录数据中心防火墙，将该终端IP加入黑名单并隔离至专用VLAN，攻击链被及时切断，核心数据未受损。该项目实现了“边界+内网”双层防护，内网横向攻击事件处置效率提升80%以上。

3 示范效应

该案例对已部署态势感知平台和数据中心防火墙但尚未有效协同的高校具有极强的示范意义。首先，凸显了数据中心防火墙在防御内网横向攻击中的不可替代性——仅靠态势感知“看得见”远远不够，必须依靠防火墙“拦得住”，而数据中心防火墙的区域隔离能力正是阻断横向移动的关键。其次，形成了“南北向+东西向”双层防御范式，为教育行业应对勒索病毒、APT内网潜伏等高级威胁提供了可复制的架构参考。

在乘数效应方面，该项目积累的安全运营日志和事件处置数据可反哺平台的机器学习模型训练，实现威胁检测能力的持续进化，形成“数据积累—模型优化—能力提升”的正向循环。该案例模式可横向推广至其他仅配备态势感知平台和数据中心防火墙的教育机构，推动教育行业数据安全治理从“设备堆砌”向“平台驱动、智能运营”的方向演进。

人脸数据安全中台教育数据安全案例

武汉学院

1 场景

高校智慧校园建设中，人脸识别已广泛应用于门禁、考勤、支付等场景，涉及上万师生。然而，人脸信息作为不可更改的生物特征，面临三大风险：一是采集无度，多部门重复采集且未获用户单独同意；二是流转无序，数据在第三方平台明文传输、违规共享；三是防护无力，存储端缺乏针对性加密，易遭拖库或内部泄露。武汉学院针对1万余名师生、日均万级的人脸比对需求，开展专项治理，通过构建“统一人脸库”与“数据安全管控平台”，解决了数据孤岛与泄露风险并存的矛盾，在提升通行效率30%的同时，将数据泄露风险降至趋近于零，兼顾《个人信息保护法》合规与业务便捷性，推动了校内人脸数据安全中台与数据治理体系的标准化建设。

2 成果呈现

武汉学院人脸安全数据中台定位为高校人脸数据的统一管控中枢，通过“统一归集、标准治理、全流程防护”，解决分散建设带来的安全与管理难题。本案例遵循“一库、一平台、三防线”的逻辑架构。打破学校各业务系统直接对接摄像头的旧模式，建立全校统一的生物特征中枢。管控中枢，通过“统一归集、标准治理、全流程防护”，解决分散建设带来的安全与管理难题。本案例遵循“一库、一平台、三防线”的逻辑架构。打破学校各业务系统直接对接摄像头的旧模式，建立全校统一的生物特征中枢。

2.1 构建校级统一人像库，解决数据分散问题

平台将分散在各业务系统中的人脸数据进行归集，形成全校统一的人脸数据源，从根本上解决校园人脸识别数据如何统一采集的问题。



统一采集入口：支持H5页面、自助采集终端等多种方式，确保师生通过规范渠道完成采集，避免重复录入。

统一数据标准：平台制定人脸数据的格式、质量、接口规范，解决多厂商、多算法之间的兼容性问题。

2.2 全生命周期安全管理，实现过程可控

平台对人脸数据从采集到销毁的每一个环节进行技术管控。采集阶段采用SSL加密传输，采集前明确告知用户使用目的、使用范围，并取得单独同意。存储使用国密算法对原始照片和特征值进行加密存储，定期备份，防止数据外泄。分发阶段针对不同应用场景，提供人像副本（添加可溯源的水印，实现人脸识别数据溯源）与特征值分发（对安全性要求较高的系统，只分发不可逆的特征值，业务端不保留原始照片，降低泄露风险）两种分发模式。销毁阶段要求所有接入系统提供数据销毁机制，用户撤回同意或数据超期后，可确保彻底清除，并且在数据整个生命周期明确告知用户使用目的。

2.3 灵活部署，适配不同业务场景

后端比对模式：用于统一身份认证等安全敏感场景，业务系统不保存人脸数据，实现人脸库与统一身份认证系统对接的集中管控。

终端比对模式：用于门禁等高并发、高可用场景，特征值下发至终端设备，解决校园人脸门禁数据同步方案中的同步效率与断网可用性问题。

3 示范效应

武汉学院人脸数据安全中台破解了“便利”与“隐私”的对立难题。对于正在全面铺开智慧校园建设的高校，提供了从“野蛮生长”到“合规精细”的转型样板。特别是针对教育部关于数据安全合规检查的要求，该模式可直接复制推广，具有先进的行业引领性。

同时通过人脸数据中台的建设倒逼学校成立数据治理机构，建立“数据资产一本账”的管理机制，对学校的管理模式变革起到了极大的促进作用。通过标准化接口的建设，规范了第三方算法厂商的接入标准，解决了多厂商算法不兼容、安全水位参差不齐的痛点，实现数据生态协同。通过公开透明的安全策略，打消了师生对于“全景式监控”的顾虑，为人脸识别技术在公共服务的合法应用树立了正面形象。

本方案最大的亮点在于从“被动合规”转向“主动防御”，确立了人脸特征数据是高校核心机密资产的管理定位，通过搭建校级人脸数据安全防护平台，与企业微信深度集成，覆盖门禁、宿舍、图书馆、教务、体测、巡课等9类场景，实现一次采集、全校通行，本地化部署、国密加密、等保三级合规，数据不出校、调用全审计。



面向数智化校园基础设施解决方案

宏杉科技

针对教育数字化转型下高校数据爆发式增长、业务场景多元化的核心需求，打造适配校园教学、管理、运维全场景的基础架构升级方案，从算力调度、核心业务支撑、非结构化数据存储到全链路数据保护，实现校园IT架构的一体化、高可靠、易扩展升级，为智慧校园建设筑牢技术底座。

1 需求与挑战

随着教育数字化转型的深入推进，高校信息化建设面临前所未有的数据增长压力：

（1）资源管理挑战：云/虚拟化平台需求升级，CPU、GPU算力需统一调度；

（2）存储可靠性挑战：校园一卡通/财务等核心业务系统需7×24小时不间断运行；

（3）海量非结构化数据存取挑战：智慧教室、教学资源库、科研数据从PB级向EB级快速演进，传统存储扩展方式受限，无法满足数据扩容需求；

（4）科研&智算领域，算力与存力严重失衡，GPU算力爆发式增长，存储性能成为关键瓶颈，导致算力空转，投入成本浪费。AI推理成本飙升，KVCache呈爆炸式增长，1个Token从字节级膨胀至MB级，显存负载万倍放大，硬件成本激增；

2 解决方案

2.1 虚拟化平台：MCloud宏杉云平台，实现GPU算力调度一体化

宏杉云作为新一代云产品，集多云管理、GPU算力调度、运维管理、运营管理等能力于一体，具备容灾、云安全等场景化方案扩展能力，可为用户提供成本可控、架构灵活、运维简单、资源统管、性能极致的私有云解决方案。

随着AI、大数据技术的普及，算力需求正呈爆发式增长，传统算力调度方案的局限性日益凸显。宏杉云管平台创新实现私有云/超融合与GPU的融合部署，打破传统方案的兼容性壁垒，已兼容国内外90%以上GPU显卡型号，提供统一的CPU与GPU算力调度能力，简化数据中心架构，降低建设成本。

在教育云场景中，面对多校区云资源分散异构、运维混乱、个性化需求突出等问题，平台不仅能实现跨校区云资源的统一管理，更通过开放API接口对接第三方系统，精准匹配高校教务、科研、后勤等多场景的个性化运维需求，让教育数字化建设更高效、更灵活。

2.2 一卡通/财务/数据库等核心业务：MS9000G3四控高端存储/双活存储解决方案

MS9000G3系列存储是宏杉科技新一代紧耦合四控高端存储。结合宏杉科技高端存储架构技术和第三代V4引擎技术，提供比传统双控存储更高的可靠性，允许任意三个控制器同时故障时数据不丢失、业务不中断，保障关键业务7×24h持续在线，为数据中心核心应用提供安全可靠、性能卓越、智能高效的存储平台。

同时，宏杉科技全系列存储产品支持双活存储解决方案，宏杉科技的对称双活存储（Symmetrical Dual Active Storage，简称SDAS）是一项专门针对双活存储方案的创新技术，无需引入任何第三方软硬件，即可通过两台同档次的MS系列存储阵列搭建双活架构，互为冗余。当其中一台存储发生故障时，另一台存储可实时接管业务，实现RPO=0、RTO=0，支持近距离和远距离的双活数据中心系统构建。

2.3 智慧教室/教学资源库：万象系列产品助力海量非结构化数据存储

随着大数据、云计算、高性能计算等新兴IT业务的应用越来越广泛，分布式存储已成为构建现代数据基础设施的核心组件。

基于深刻的市场洞察与技术积累，宏杉科技自主研发的万象MC27000分布式存储产品与解决方案已日趋完善。旨在系统性解决企业运营和生产过程中各类业务产生的非结构化数据的存储、共享、安全、扩展、性能、可管理性等方面的关键需求，更能为教育行业提供完全自主可控的专属存储方案，精准适配智慧校园建设场景。

海量吞吐，录播无忧：单节点带宽可达上百GB/s，提供TB级聚合访问带宽，轻松支撑全校千路高清录播并发写入与万人在线点播，确保教学视频“存得下、播得顺”。

◉ 极致性能，微秒时延：单节点可提供200万IOPS与120GB/s最大访问带宽，全面支持文件协议与块协议，实现端到端RDMA，将数据访问时延压缩至微秒级，轻松应对大模型训练、深度学习推理等高并发、高吞吐科研场景，让GPU彻底告别等待，全力释放算力价值。

◉ 先进介质，智能分层：兼容高性能NVMe SSD与大容量SAS/NL-SAS盘，最大可支持3200块硬盘；搭配自动分层技术，智能识别并调度热、温、冷科研数据，在保障核心业务极致性能的同时，有效控制存储成本，让每一分科研投入都实现价值最大化。稳定可靠，业务永续：采用控制器双活高可用设计，结合RAID技术与全局热备盘，确保科研数据万无一失；搭配快照、克隆、异步复制等全方位数据保护功能，为AI训推、科研数据处理的长久稳定运行提供坚不可摧的保障，避免科研数据丢失或业务中断造成的损失。

◉ AI赋能，记忆持久化：MSCache键值缓存调度系统是Alpha700实现“以存强算”的关键创新。作为GPU集群与存储系统之间的智能缓存层，MSCache通过搭建可扩展的PB级专属缓存空间，大幅提升KV Cache驻留量与缓存命中率，减少GPU冗余计算，实现双重核心收益：一是显著降低推理时延，让大模型响应更流畅，适配科研场景下多轮对话、长上下文的推理需求；二是减轻GPU工作负载，使同等规模的GPU集群可支持更高用户并发、处理更长上下文，直接降低科研机构的AI推理硬件投入与运营成本。目前已深度适配DeepSeek、通义千问等主流大模型，开箱即用，无需复杂二次开发，可快速部署落地，让AI智慧真正服务于科研一线。

3 用户价值

◉ 打破多云管理壁垒

云管平台以自主可控的核心技术、业内领先的纳管能力，为用户打破多云管理壁垒，降低运维成本，释放云资源价值。

◉ 业务连续性保障

确保核心系统7×24小时稳定运行，数据零丢失

◉ 教学体验提升

支撑智慧教室常态化录播数据，改善师生教学体验，MC27000-MOFS的EB级存储容量与千亿级文件支持，轻松承载海量数据爆发式增长，自动分层与多协议互访功能，简化数据管理流程，降低运维负担；

◉ 破解痛点，保障科研顺畅推进

解决算力与存力失衡、混合带宽性能矛盾、海量数据管理复杂等科研核心痛点：Alpha700的微秒级时延、高IOPS与高带宽，完美匹配GPU集群算力需求，让算力不再空置；

KV缓存调度系统，大幅减少GPU冗余计算，降低推理时延的同时，让同等GPU集群可承载更高并发、更长上下文任务，直接减少科研机构GPU硬件投入与运营成本。

◉ 未来演进无忧

弹性架构支撑未来5-10年业务发展，保护IT投资。

武汉市网络安全协会服务指南

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。

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。

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。

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。

资质认证

1、IS0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

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

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。

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!

入会流程

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