天津市人民代表大会常务委员会公告

第五十四号

《天津市网络安全和信息化条例》已由天津市第十八届人民代表大会常务委员会第二十四次会议于2026年3月27日通过,现予公布,自2026年5月1日起施行。

天津市人民代表大会常务委员会

2026年3月27日

天津市网络安全和信息化条例

(2026年3月27日天津市第十八届人民代表大会常务委员会第二十四次会议通过)

目 录

第一章 总 则

第一条 为了保障网络安全,促进信息化发展,维护国家安全和社会公共利益,保护公民、法人和其他组织的合法权益,推动高质量发展,根据《中华人民共和国网络安全法》等有关法律、行政法规,结合本市实际,制定本条例。

第二条 本市行政区域内的网络运行安全、网络信息安全以及促进信息化发展等活动,适用本条例。

第三条 本市网络安全和信息化工作坚持中国共产党的领导,贯彻总体国家安全观,坚持网络安全与信息化发展并重,遵循统筹规划、融合创新、开放共享、保障安全、赋能发展的原则,提升网络安全保护能力和信息化发展水平。

第四条 市和区人民政府应当将网络安全和信息化工作纳入国民经济和社会发展规划,制定并组织实施网络安全和信息化发展政策措施。

第五条 市和区网信部门负责本行政区域内网络安全和信息化发展工作的统筹协调和相关监督管理工作。

发展改革、教育、科学技术、工业和信息化、公安、市场监督管理、政务服务、数据管理、国家安全、密码管理、通信管理等有关单位,按照各自职责做好网络安全和信息化相关工作。

第六条 市网信部门应当按照国家有关规定,根据国家网络安全和信息化发展规划以及本市国民经济和社会发展规划,组织编制本市网络安全和信息化发展规划,报市人民政府批准后实施。

第七条 本市加强与北京市、河北省在信息化发展领域的合作,在网络互通、资源共享、服务协同等方面开展协同联动,加强网络安全和工业互联网等重点产业链分工协作,优化区域产业布局,以信息化、数智化赋能区域高质量发展。

第八条 本市加强网络安全宣传教育和信息化知识普及,提高全社会信息技术应用水平,促进全民数字素养与数字技能提升。

市和区人民政府及其有关部门应当经常性组织开展网络安全宣传教育活动,指导、督促有关单位,充分调动社会各界力量做好网络安全宣传教育工作,提升全社会网络安全意识和防护技能。

广播、电视、报刊、网络媒体等应当有针对性地面向社会进行网络安全宣传教育。

第九条 本市对在促进网络安全和信息化发展中取得突出成绩的单位和个人,按照国家有关规定,给予表彰和奖励。

第二章 网络运行安全

第十条 本市建立健全网络安全保障工作体系,加强网络安全风险防范、监测预警、应急处置等工作,防范和处置网络安全风险,提升网络安全保护能力,保障网络、关键信息基础设施、重要信息基础设施和数据的安全。

第十一条 本市按照国家规定,实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求,履行安全保护义务,保障网络免受干扰、破坏或者未经授权的访问,防止网络数据泄露或者被窃取、篡改,并加强对其用户发布信息的管理。

第十二条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序;发现其网络产品、服务存在安全缺陷、漏洞等风险时,应当立即采取补救措施,按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者在规定或者当事人约定的期限内,应当为其产品、服务持续提供安全维护。

第十三条 网络运营者部署使用人工智能等新技术新应用,应当做好安全测试和评估。新技术新应用服务提供者应当提供安全、稳定、持续的服务,保障用户正常使用。鼓励采用安全可信的芯片、软件、工具、算力和数据资源。

第十四条 本市按照有关法律、行政法规对关键信息基础设施予以重点保护。

本市在网络安全等级保护制度的基础上,对未列入关键信息基础设施的重要信息基础设施加强保护。重要信息基础设施的认定规则、具体范围和安全保护办法,由市网信部门会同有关行业和领域的主管部门、监督管理部门制定。

第十五条 网信部门会同有关行业和领域的主管部门、监督管理部门指导推动重要信息基础设施运营者,在网络安全等级保护和密码规范应用要求的基础上强化对重要信息基础设施的防护。

网信部门应当统筹协调有关部门建立重要信息基础设施网络安全信息共享机制,对重要信息基础设施的安全风险开展抽查检测并提出改进措施,对涉及重要信息基础设施的网络安全事件应急处置与网络功能恢复等,提供技术支持和指导。

第十六条 网信部门统筹协调公安机关、国家安全机关以及相关部门建立健全网络安全监测预警和信息通报机制,加强网络安全信息收集、分析和通报工作,按照规定统一发布网络安全监测预警信息,发现问题及时督促有关单位整改。

第十七条 网信部门应当协调有关部门建立健全网络安全风险评估和应急工作机制,制定网络安全事件应急预案,并定期组织演练。

网络运营者应当制定网络安全事件应急预案,及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险;发生危害网络安全的事件时,网络运营者应当立即启动应急预案,采取相应的补救措施,消除安全隐患,防止危害扩大,并及时向社会发布与公众有关的警示信息。

发生较大以上网络安全事件时,网络运营者应当按照有关规定,向网信、公安等部门报告。网信部门应当会同有关部门对网络安全事件及时进行处置,能源、电信等单位应当为网络安全事件应急处置与网络功能恢复提供相应保障和支持。

第十八条 市和区人民政府应当支持网络安全技术的研发和应用,支持工业互联网安全、人工智能安全、车联网安全、商用密码等领域技术创新,支持高等学校、科研院所、企业联合开展关键技术攻关,推进新技术应用网络安全共性基础平台建设,推广安全可信的网络产品和服务。

市和区人民政府应当加大网络安全场景供给,引导产业集聚,推动网络安全教育、技术、产业融合发展。

第十九条 本市推进网络安全社会化服务体系建设,鼓励有关企业、机构依法开展网络安全认证、检测和风险评估等安全服务,提高网络安全保护水平。

第三章 网络信息安全

第二十条 本市加强网络信息安全保障,依法规范网络数据处理活动,强化个人信息保护和网络信息内容管理,深化网络生态治理。

第二十一条 任何组织和个人不得利用网络数据从事非法活动,不得从事窃取或者以其他非法方式获取网络数据、非法出售或者非法向他人提供网络数据等非法网络数据处理活动。

第二十二条 网络数据处理者应当依照法律、行政法规的规定和国家标准的强制性要求,在网络安全等级保护的基础上,采取措施加强网络数据安全防护,建立健全网络数据安全管理制度,对所处理网络数据的安全承担主体责任。

本市按照数据分类分级保护制度的要求,对列入重要数据目录和重要数据具体目录的网络数据进行重点保护。重要数据的网络数据处理者应当明确网络数据安全负责人和管理机构,依法履行网络数据安全保护责任。

第二十三条 网络数据处理者向境外提供数据的,应当遵守法律、法规的规定,履行数据安全保护义务,采取技术措施和其他必要措施,保障数据出境安全。发生或者可能发生数据安全事件的,应当采取补救措施,及时向市网信部门和其他有关主管部门报告。

第二十四条 利用网络处理个人信息应当遵循合法、正当、必要和诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。

处理个人信息应当具有明确、合理的目的,并应当与处理目的直接相关,采取对个人权益影响最小的方式。收集个人信息,应当限于实现处理目的的最小范围,不得过度收集个人信息。

除法律、行政法规另有规定外,处理个人信息应当取得个人同意。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的,从其规定。

第二十五条 网络数据处理者应当采取技术措施和其他必要措施,确保其收集、存储的个人信息安全。发生或者可能发生个人信息泄露、篡改、丢失的,应当立即采取补救措施,按照规定及时告知个人并向有关部门报告。

网络数据处理者应当定期自行或者委托专业机构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。

第二十六条 本市倡导诚实守信、健康文明的网络行为,强化网络内容建设和管理,鼓励制作、发布、传播含有解读中国特色社会主义道路、理论、制度、文化,弘扬社会主义核心价值观、展示高质量发展成就、宣传中华优秀传统文化和时代精神,以及其他讴歌真善美、促进团结稳定等内容,推动形成全社会健康文明用网的良好氛围。

第二十七条 本市深化网络信息内容生态治理,依法处置违法信息和不良信息,规范网络传播秩序,营造清朗网络空间。

第二十八条 生成式人工智能服务提供者应当依法承担网络信息内容生产者责任,履行网络信息安全义务。涉及个人信息的,依法承担个人信息处理者责任,履行个人信息保护义务。

第二十九条 提供生成式人工智能服务的网络数据处理者应当加强对训练数据和训练数据处理活动的安全管理,采取有效措施防范和处置网络数据安全风险。

第四章 信息化发展

第三十条 本市推进信息化发展,以数字化、智能化转型升级为重点,推动信息技术在农业、制造业、服务业以及政务服务、社会民生等领域的应用场景建设和融合创新,培育壮大信息产业和数字经济,发挥信息化对经济社会发展的驱动引领作用,因地制宜发展新质生产力。

第三十一条 市和区人民政府应当加强对信息化工程的统筹规划和监督管理。

有关部门审查政府投资的信息化工程项目,应当对项目是否符合国家和本市网络安全和信息化发展规划、技术标准和规范、信息安全保障和信息资源共享等要求进行审查。

非政府投资的重大公共基础性信息化工程或者网络安全工程项目,应当符合国家和本市网络安全和信息化发展规划、技术标准和规范等要求。建设单位在依法办理相应手续后,应当向网信部门备案。

第三十二条 市和区人民政府及其有关部门应当大力完善新一代移动通信技术、高速光纤网络等通信网络基础设施,加快建设通用算力、超级算力、智能算力等协同发展的算力基础设施,支持工业互联网、人工智能、区块链、车联网等融合创新基础设施建设。

鼓励高等学校、科研院所、企业等参与网络安全和信息化领域国家重大科技基础设施和重大创新平台建设。

第三十三条 市和区人民政府及其有关部门应当鼓励支持相关企业、科研院所、高等学校加强对集成电路、人工智能、基础软件、新一代通信技术等关键核心技术攻关,加强量子信息、脑机接口、数字孪生、低空安全等前沿信息技术布局。

第三十四条 市和区人民政府及其有关部门应当采取措施加快场景培育和开放,支持建设综合性重大场景、行业领域集成式场景、高价值小切口场景,鼓励和支持信息化领域新技术、新产品、新业态利用场景资源进行产业化应用,推动信息技术创新和成果转化。

第三十五条 市和区人民政府及其有关部门应当制定完善促进信息产业发展的政策,统筹规划信息产业布局,鼓励企业在信息技术和产品研发、应用示范、成果转化和产业化发展方面发挥主体作用,推动新一代信息技术创新应用产业集群建设,促进电子信息产品制造、软件开发和信息技术服务等信息产业高质量发展。

第三十六条 市和区人民政府及其有关部门应当积极推进信息资源整合、共享和开放,支持信息资源的公益性开发利用,引导个人和组织开发信息资源。

第三十七条 市和区人民政府及其有关部门应当加快农业农村信息基础设施建设,推广信息技术在农业农村生产经营、公共服务、生态保护、乡村治理等方面的应用,发展智慧农业,推进数字乡村建设。

第三十八条 市和区人民政府及其有关部门应当加快推进新一代信息技术与制造业深度融合,坚持数字化赋能,扩大制造业设备更新和技术改造投资,促进智能制造发展,推进制造业数字化转型、网络化协同、智能化变革。

第三十九条 市和区人民政府及其有关部门应当采取措施加强服务业信息化应用,支持数字赋能现代服务业,丰富民生保障、教育医疗、文旅商贸、金融保险、交通物流等数字化应用场景,推动生活性服务业向高品质和多样化转型升级,发展科技服务、工业设计、软件和信息服务等生产性服务业,促进现代服务业高质量发展。

第四十条 本市加快数字化绿色化协同转型发展,发展数字和绿色的融合新技术和产业体系,深化人工智能、大数据、云计算、工业互联网、物联网等在电力能源系统、工农业生产、交通运输、建筑建设、城市运行管理、生态环境治理等领域的应用,以数字化智能化赋能产业绿色化转型。

第四十一条 市和区人民政府及其有关部门应当落实数字政府建设的要求,统筹推进政务基础设施集约智能、自主可控,将数字技术广泛应用于政府管理服务,推动政府治理流程优化、模式创新和履职能力提升,推进行政决策科学化、社会治理精准化、公共服务高效化,打造协同高效的数字政府服务体系。

第四十二条 本市加强数字知识和技能普及,推动数字教育资源、数字技能培训、数字产品和信息服务高质量发展和开放共享,面向公众推广和普及就业、就医、消费、商务、金融、网络安全、个人信息保护等领域数字知识技能,推动优化数字生活环境、提高数字生活品质。

鼓励为老年人、残疾人等群体提供有针对性的生产生活实用信息服务。

第五章 保障措施

第四十三条 本市加强对网络安全和信息化发展的资金支持。市和区人民政府应当加大投入,统筹使用各类产业发展、科技创新等政策资金,支持网络安全和信息化相关产业和重点项目,支持网络安全和信息化技术的研究开发和应用。

引导和支持社会资金投资网络安全和信息化建设。

第四十四条 市市场监督管理部门、网信部门和有关部门依据各自职责,推动制定有关信息化发展要求的标准并监督实施。

鼓励和支持高等学校、科研院所、行业协会、产业联盟、企业等参与网络安全国家标准、行业标准和信息化标准的制定工作。

第四十五条 市和区人民政府及其有关部门应当加强网络安全和信息化相关知识产权保护,支持企业创新发展和产业转型升级。

支持企业、高等学校、科研院所等各类创新主体围绕网络安全和信息化技术创新加强知识产权创造,培育和形成知识产权成果,推动知识产权在网络安全和信息化领域的转化应用。

第四十六条 市教育、科技、网信等部门应当支持高等学校、科研院所等加强网络安全和信息化基础研究、应用研究,促进高等学校、科研院所开展跨学科、跨专业研究,支持高等学校加强计算机科学与技术、网络空间安全、密码科学与技术、电子信息等网络安全和信息化基础学科建设,优化前沿交叉学科布局,搭建交叉学科发展平台,支持建设国家一流网络安全学院。

第四十七条 本市加强网络安全和信息化人才队伍建设,强化网络安全和信息化人才的培养和引进。

鼓励高等学校、科研院所、职业教育培训机构等按照用人单位和市场的实际需求,采取多种形式培养实用型和创新型的网络安全和信息化人才,加强交叉学科人才培养。支持用人单位加强本单位网络安全和信息化人才的继续教育和在职培训,提高网络安全和信息技术应用和管理水平。

人力资源和社会保障部门、网信部门应当支持用人单位根据网络安全和信息化发展需要,引进实用型和创新型人才。

第四十八条 网络安全和信息化相关行业组织按照章程,加强行业自律,指导会员加强网络安全保护,推动信息技术应用,开展学术交流和科普教育,参与政策咨询和标准制定,促进行业健康发展。

第四十九条 本市建立网络安全和信息化专家咨询制度。网络安全和信息化的重大决策、规划编制、标准制定、重大项目建设,应当经过专家论证或者听取专家咨询意见。

第六章 法律责任

第五十条 网信部门以及有关部门在履行网络安全和信息化监督管理职责中,发现网络或者数据处理活动存在较大安全风险或者可能发生安全事件的,可以按照法定的权限和程序对有关单位和个人进行约谈,指出存在的问题,提出整改要求。被约谈的单位和个人应当按照要求采取措施,及时整改,消除隐患。

第五十一条 网信部门、有关部门及其工作人员违反本条例规定,不履行职责或者不正确履行职责的,对直接负责的主管人员和其他直接责任人员依法给予处分;构成犯罪的,依法追究刑事责任。

第五十二条 违反本条例规定的行为,法律、行政法规已有处理规定的,从其规定。

第七章 附 则

第五十三条 本条例自2026年5月1日起施行。2007年9月12日天津市第十四届人民代表大会常务委员会第三十九次会议通过的《天津市信息化促进条例》同时废止。

惩治"机闹"犯罪 两高发文守护民航飞行平安

民航安全无小事,法治之力护平安。

4月8日,最高人民法院、最高人民检察院联合发布办理危害民航飞行安全刑事案件的司法解释,用严明的法律标尺衡量行为边界,守护飞机上万千乘客的安全。

依法惩治"机闹"犯罪行为——

违规开启民航飞机应急出口舱门,在机舱内打架斗殴,对乘务人员使用暴力……这些行为严重影响飞行安全。

如何判定这些行为属于行政违法行为,还是构成刑事犯罪?

对此,司法解释明确,在民航飞机处于依靠自身动力移动期间或者空中飞行期间违规开启舱门、足以引发危害公共安全危险的情况下,以刑法中的"以危险方法危害公共安全罪"定罪处罚;对于飞机尚未依靠自身动力移动等情况下违规开启舱门的行为,可以根据有关规定给予行政处罚,并由行为人承担相应的民事赔偿责任。

最高法刑四庭庭长罗国良介绍,司法解释采用列举式规定,对在飞行中的民航飞机上使用暴力行为构成暴力危及飞行安全罪的定罪量刑标准作出了规定,特别明确乘务员即通常所称的"空姐空少"属于"飞行安全保障人员",是暴力危及飞行安全罪的犯罪对象,对飞机乘务员使用暴力的行为可能构成暴力危及飞行安全罪。

从严惩治"造谣"涉民航飞行安全犯罪——

口无遮拦谎称"飞机有炸弹",会有哪些严重后果?

2023年8月,陈某波的妻女因超过值机时间而未能登机。陈某波同日报警要求为其妻女办理机票改签,未果后心生不满,在报警电话中编造航班上有炸弹的虚假恐怖信息,导致机场启动一级应急预案,后续多个航班延误。最终,陈某波以编造虚假恐怖信息罪被判处有期徒刑一年。

陈某波虽被依法惩处,但在司法解释出台前,相关法律适用问题比较复杂,编造、故意传播涉民航飞行安全虚假恐怖信息在什么情况下可以判处五年以上有期徒刑没有明确标准,影响执法司法实践中对此类行为打击的精准度和惩治的威慑力。

对此,司法解释突出对编造、故意传播涉民航飞行安全虚假恐怖信息犯罪的从严惩治,规定行为人的行为影响民航航班、民用机场正常运行,或者致使公安、武警、消防救援、卫生检疫等部门采取应对措施的,应作犯罪处理;结合民航飞行安全领域的实际情况及危害行为的特点,明确列举六种情形,具有这六种情形的,属于造成严重后果,处五年以上有期徒刑。刑事惩处更为严格了。

司法解释同时明确,无论是采取明示还是暗示的方式编造、故意传播涉民航飞行安全虚假恐怖信息,符合相关条件的,均可构成编造、故意传播虚假恐怖信息罪。

坚持依法从严,贯彻宽严相济刑事政策——

编造、故意传播涉民航飞行安全虚假恐怖信息行为严重影响社会公众安全感和民航行业健康发展,甚至可能造成一定范围内的社会恐慌心理,必须坚持依法从严惩处总体原则不动摇。

据介绍,对出于仇视报复社会等动机和目的,经周密预谋策划后实施编造、故意传播涉民航飞行安全虚假恐怖信息行为,意图制造社会不稳定因素的行为人,以及多次实施此类行为屡教不改的行为人,依法予以严惩。对于行为情节一般,且具有自首、坦白、认罪认罚等法定或者酌定从宽处罚情节的行为人,可以依法适度予以从宽处理,确保罪责刑相适应。

民航飞行安全底线不容触碰。人人都应敬畏法律、遵守规则、文明出行,共同维护民航飞行安全和社会公共安全,让每一次起降都顺利、平安。

新华社北京4月8日电

我国将健全完善较大亡人火灾备案审查制度

据新华社北京4月8日电 火灾事故调查处理是推动消防安全治理模式向事前预防转型的重要手段。记者8日从国家消防救援局获悉,我国将健全完善较大亡人火灾备案审查制度,坚决防止火灾事故重蹈覆辙。

日前印发的《关于加强基层消防工作的意见》明确提出,消防部门依法开展火灾事故调查处理工作。国家消防救援局消防监督司副司长王天瑞表示,从今年起,对每起较大亡人火灾,国家消防救援局将启动协作机制,调派专家参与指导,各地较大火灾事故调查报告审议前报国家消防救援局审查,严防调查浮于表面、问责蜻蜓点水、警示通报秘而不宣,坚决防止事故大事化小、小事化了,甚至避重就轻,确保调查质效。

此外,我国还将健全以吸取教训为导向的一般火灾调查机制。对于大量一般火灾事故,强化技术及管理责任调查,查清直接原因、事故责任,提高调查效率,节约调查成本,通过调查出台管用措施,织密管理制度,修订完善标准。

对每起重大亡人火灾,国务院安委会将实行挂牌督办,国家消防救援局将派出现场督办组,调派全国专家骨干全程参与指导。同时,对性质严重、造成重大社会影响的火灾事故实行提级调查。调查结案后,在向社会公布火灾调查报告的同时,还将公布火灾的真相和细节。

金融监管总局发文 部署2026年金融支持乡村全面振兴

拓展首贷户 坚决防止并纠正"内卷式"竞争行为

据新华社北京4月8日电 国家金融监督管理总局4月8日对外发布通知明确,2026年农业发展银行、大中型商业银行要继续单列涉农信贷计划,努力实现同口径涉农贷款余额较年初持续增长目标。

《关于做好2026年金融支持乡村全面振兴工作的通知》明确,2026年,引导大中型银行积极发展农业产业链金融,拓展首贷户,以改革促农村中小银行支农支小能力提升,合理确定普惠型涉农贷款内部倾斜政策,坚决防止并纠正"内卷式"竞争行为。

通知要求,优化涉农信贷产品和服务,结合"三农"特点提供更为适配的信贷产品,依法合规加大对涉农企业和农户贷款展期、续贷支持力度。强化稻谷、小麦、玉米、大豆保险保障,因地制宜发展地方优势特色农产品保险。发挥农业保险在防灾减灾中的作用。