目　录

（内部会员资料，无偿提供，每两个月寄送一次）

典 型 案 例

陈某某诉某科技公司公路旅客运输合同纠纷案

【基本案情】

某科技公司系某网约车平台的经营者。唐某某系网络预约出租汽车驾驶员。乘客陈某某通过某网约车平台预约下单乘坐唐某某驾驶的网约车。驾驶过程中，因唐某某操作不当，车辆撞向路边护栏，造成陈某某右手粉碎性骨折。公安交管部门认定，唐某某在驾驶过程中操作不规范，负事故全部责任。陈某某诉至法院，请求判令某科技公司赔偿各项经济损失共计人民币 26 万余元。

【裁判结果】

审理法院认为，《网络预约出租汽车经营服务管理暂行办法》第十六条规定，网约车平台公司承担承运人责任，应当保证运营安全，保障乘客合法权益。本案中，陈某某通过某科技公司的网约车平台发出出行信息，该平台通过短信提示乘坐车牌号码和联系电话接受要约，可以认定双方之间形成了公路旅客运输合同关系。根据《中华人民共和国民法典》第四百六十五条、第八百一十九条、第八百二十三条规定，某科技公司作为承运人应当对运输过程中旅客的伤亡承担赔偿责任，在没有证据证明陈某某的受伤是其自身健康原因或故意、重大过失造成的情况下，陈某某的损失应由某科技公司承担。结合误工费等赔偿项目的计算标准，最终判决：某科技公司赔偿陈某某各项损失共计 23 万余元。

【典型意义】

近年来，随着网约车行业的快速兴起，网约车已成为社会公众日常出行的重要选择。网约车平台公司作为承运人，应当保障乘客的乘车安全。本案判决认定乘客和网约车平台公司成立公路旅客运输合同关系，依法判令网约车平台公司对车辆运营过程中发生的乘客损害承担赔偿责任，既合理认定事故责任，妥善处理事故纠纷，也督促网约车平台加强安全管理，提升服务质量，为乘客提供更便捷、可靠的出行体验，守护网约车安全运营底线。

周某某诉陈某、辛某某、某保险公司等机动车交通事故责任纠纷案

【基本案情】

辛某某驾驶机动车载客，未紧靠道路右侧停车，乘客陈某开门时也未充分注意，与骑电动自行车的周某某发生碰撞，造成周某某受伤，车辆受损。公安交管部门认定，辛某某负事故主要责任，陈某负事故次要责任，周某某无责任。辛某某驾驶的车辆在某保险公司投保了交强险和商业三者险，事故发生在保险期间内。周某某诉至法院，请求判令陈某、辛某某、某保险公司赔偿损失。

【裁判结果】

审理法院认为，根据《中华人民共和国民法典》第一千二百一十三条的规定，机动车发生交通事故造成损害，属于该机动车一方责任的，先由交强险在责任限额范围内予以赔偿；不足部分，由承保机动车商业保险的保险人按照保险合同的约定予以赔偿；仍然不足的，由侵权人赔偿。本案中，辛某某未紧靠道路右侧停车，陈某开车门未确保安全，造成周某某受损，二人行为共同造成了损害后果。对于受害人而言，机动车一方系一个整体，陈某与辛某某同属机动车一方，陈某的责任也属于机动车一方责任，某保险公司关于其对乘客责任部分不应承担保险责任的抗辩不能成立，某保险公司应在交强险和商业三者险范围内承担全部赔偿责任。就超出保险赔付范围的部分，由驾驶人辛某某承担 70%赔偿责任，乘客陈某承担 30%赔偿责任。最终判决：某保险公司赔偿周某某各项损失共计 24 万余元，辛某某赔偿周某某 4200 元，陈某赔偿周某某 1800 元。

【典型意义】

日常生活中，车内人员疏于观察，贸然打开车门与他人发生碰撞造成交通事故，俗称“开门杀”。该类事故通常因疏忽导致，但往往造成他人人身财产损害，有些甚至引发人身伤亡等严重后果。本案判决明确，在“开门杀”事故中，保险公司应在交强险和商业三者险范围内，就驾驶人和乘客的责任承担保险赔偿责任，其余部分由驾驶人、乘车人依法承担。本案判决既充分发挥保险保障作用，及时救济受害人，又强化驾驶人、乘车人安全责任意识，警示驾驶人、乘车人均应严格遵守交通规则，谨慎注意，避免小疏忽引发大事故。

赵某诉钱某机动车交通事故责任纠纷案

【基本案情】

钱某驾驶机动车搭载赵某回村途中，车辆撞到路中的障碍物，失控撞向路边灯柱发生交通事故，造成赵某受伤。公安交管部门认定，钱某负事故全部责任。赵某诉至法院，请求判令钱某赔偿医疗费、残疾赔偿金、精神损害抚慰金、误工费等损失共计 19 万余元。

【裁判结果】

审理法院认为，根据《中华人民共和国民法典》第一千二百一十七条的规定，非营运机动车发生交通事故造成无偿搭乘人损害，属于该机动车一方责任的，应当减轻其赔偿责任，但是机动车使用人有故意或者重大过失的除外。本案中，赵某系无偿搭乘钱某驾驶的车辆。虽然公安交管部门认定钱某承担事故全部责任，但判断钱某是否存在故意或重大过失，还应综合事故发生原因、损害后果等因素予以确定。本案中，钱某具有驾驶案涉车辆的相应驾驶资格，亦不存在酒后驾驶等法律禁止驾驶的行为。本案事故发生在凌晨，当时公路上有障碍物，灯光对于驾驶员判断路面障碍物并及时避让有一定影响。此外，赵某在车辆后排乘坐但未系安全带对损失的扩大也有过错。钱某无偿搭载赵某属于利他性的行为，对其过失行为不应过分苛责。综合以上情况，钱某的行为不属于《中华人民共和国民法典》第一千二百一十七条规定的机动车使用人有重大过失的情形，可以减轻钱某的赔偿责任。最终判决：钱某对赵某的损失承担 70%的赔偿责任。

【典型意义】

《中华人民共和国民法典》第一千二百一十七条规定“好意同乘”情形下应减轻机动车一方的赔偿责任。这对促进形成互助友爱社会风尚具有积极意义，也符合绿色低碳出行方式的倡导。实践中，公安交管部门出具的事故责任认定书，对于全责、主责、次责等的认定，通常是结合对事故各方的过错比较作出。在“好意同乘”情形下，驾驶人是否构成重大过失，进而能否减轻责任，仍需结合全案事实进行评判。本案判决综合考虑事故责任认定书、事故发生原因、损害后果等因素，依法减轻驾驶人的赔偿责任，有利于维护友善互助的传统美德，也警示驾驶人和乘车人共同遵守交通规则，驾驶人需谨慎驾驶，乘车人也需遵守相关规定，做好系安全带等风险防范措施。

王某诉刘某、某保险公司等机动车交通事故责任纠纷案

【基本案情】

王某驾驶电动自行车与刘某驾驶的机动车发生交通事故，造成车辆损坏，王某受伤。公安交管部门认定，刘某负事故主要责任，王某负事故次要责任。刘某驾驶的机动车在某保险公司投保了交强险及商业三者险，事故发生在保险期间内。事故发生后，依抢救中心申请，路救基金垫付王某医疗费 19 万余元。王某诉至法院，请求判令刘某、某保险公司赔偿各项损失。本案审理过程中，路救基金管理机构请求法院对其垫付的医疗费一并处理。

【裁判结果】

审理法院认为，我国设立路救基金的目的系为保障交通事故中受害人的医疗抢救费用，从而使受害人得到及时救治。根据《中华人民共和国民法典》第一千二百一十六条、《中华人民共和国道路交通安全法》第七十五条的规定，路救基金先行垫付部分或全部抢救费用后，其管理机构有权向交通事故责任人追偿。据此，本案一并处理路救基金垫付医疗费后的追偿问题，于法有据。最终判决：某保险公司赔偿王某 160 万余元；刘某赔偿王某 45 万余元；路救基金管理机构先行垫付的医疗费，由刘某投保的保险公司向其支付。

【典型意义】

路救基金是依法筹集用于垫付道路交通事故中受害人人身伤亡的丧葬费用、抢救费用的社会专项基金，其目的在于保障道路交通事故中受害人的合法权益，在肇事机动车不明、未参加强制保险或抢救费用超过机动车强制保险责任限额，需要支付受害人抢救、丧葬等费用的特定情形下，为受害人提供及时救助。路救基金管理机构基于其垫付行为，依法享有追偿权。本案在路救基金垫付受害者抢救费用后，在机动车交通事故责任纠纷案件中对路救基金管理机构的追偿权诉请依法一并处理，不仅有利于保障路救基金的正常运转，也有利于一次性解决纠纷、减轻当事人诉累，从而实现交通事故的快速、妥善处理。

颜某诉某超市产品责任纠纷案

【基本案情】

2025 年 4 月 22 日，颜某在接未成年子女放学时，在学校附近某超市花费 4 元为子女购得零食 1 袋。食品包装上记载生产日期为 2024 年 7 月 12 日，保质期为 9 个月。颜某发现自己买到了过期零食并要求某超市赔偿未果，遂起诉请求某超市返还货款 4 元，支付惩罚性赔偿金 1000 元。

【裁判结果】

法院经审理认为，《中华人民共和国食品安全法》第 67 条规定，预包装食品的包装上应当有标签，标签应当标明生产日期和保质期；专供婴幼儿和其他特定人群的主辅食品，其标签还应当标明主要营养成分及其含量。第 148 条第 2 款规定：“生产不符合食品安全标准的食品或者经营明知是不符合食品安全标准的食品，消费者除要求赔偿损失外，还可以向生产者或者经营者要求支付价款十倍或者损失三倍的赔偿金；增加赔偿的金额不足一千元的，为一千元。但是，食品的标签、说明书存在不影响食品安全且不会对消费者造成误导的瑕疵的除外。”某超市将超过保质期的食品销售给颜某，属于销售明知不符合食品安全标准食品的行为，应当承担惩罚性赔偿责任。因按价款十倍计算的赔偿金不足 1000 元，应按 1000 元计算惩罚性赔偿金。据此，判决某超市退还颜某货款 4 元，另赔偿颜某 1000 元。

【典型意义】

中小学生对不符合食品安全标准食品的判别力较弱、维权意识相对淡薄、维权能力不足，即使购买到超过保质期的食品、“三无食品”也不能准确判别，甚至没有判别的意识，成为食品安全问题的“易受害群体”。个别商家利用中小学生认知能力不足、维权意识薄弱的特点，将超过保质期食品等存在安全隐患的食品在校园周边出售，损害广大中小学生的身体健康。本案系学生家长购买食品后发现过期索赔被拒才提起诉讼，虽然学生家长只购买了 4 元零食，但审理法院依照惩罚性赔偿金最低为 1000 元的规定，判决经营者承担赔偿责任，让违法经营者得不偿失。该判决充分发挥惩罚性赔偿责任的惩治作用，提高违法成本，有力震慑在校园周边向学生出售超过保质期食品等违法行为，有利于营造学生安全、家长放心的消费环境。

某农业公司诉某县市场监督管理局行政处罚案

【基本案情】

2021 年 8 月，某农业公司通过招投标获得某县中小学、幼儿园大米配送资格。因自身生产、配送能力不足，某农业公司委托某米业公司实际生产、配送大米，并向其提供了标注虚假产地的包装袋。在生产过程中，因喷码设备及印油问题，导致生产的 910 袋大米生产日期模糊不清、无法辨识。该批问题大米被配送至 8 所学校。某县市场监督管理局在检查中发现某农业公司供应的大米存在生产日期模糊及产地标注不实问题，于 2022 年 2 月作出《行政处罚决定书》，没收其违法所得，并处罚款 10 万元（某米业公司已被另案处罚）。某农业公司不服，提起本案行政诉讼，请求法院判决撤销上述《行政处罚决定书》。

【裁判结果】

法院经审理认为，涉案大米包装袋标示的生产日期模糊不清、无法辨识，违反了《中华人民共和国食品安全法》第 71 条第 2 款关于标签应清晰、醒目的规定。虽然生产日期模糊的直接原因是受托方某米业公司的设备及耗材问题，但作为委托生产方，某农业公司对受托方的生产行为负有监督责任，存在监督过失。同时，涉案大米实际产地与某农业公司提供的包装袋标示产地不符，构成虚假标示产地的违法行为。某农业公司的上述违法行为并非标签瑕疵，存在主观故意，不符合免予处罚的条件。某县市场监督管理局作出的处罚决定证据确凿，适用法律正确，符合法定程序。据此，判决驳回某农业公司的诉讼请求。

【典型意义】

校园食品安全直接关系广大师生身体健康和生命安全，是食品安全监管的重中之重。涉案食品供应对象均为中小学校和幼儿园，属于特殊消费群体，食品安全风险防控丝毫不容松懈。食品生产日期模糊导致无法判断保质期、产地虚假标注误导产品来源，均严重损害了消费者的知情权和选择权。本案特别指出委托方对受托方的生产行为负有监督责任，需对受托方的标签违法行为承担相应法律责任，有效厘清了委托生产中责任主体的认定难题，压实了委托生产的责任链条，倒逼企业建立从原粮采购、委托加工到标签设计的全链条管控机制，从源头防范食品安全风险。尤为关键的是，法院判决支持行政机关在校园食品供应领域落实最严格的监管，严防企业规避对校园食品安全的高标准要求，为市场主体划清了“校园食品无小事、合规经营是底线”的红线。该判决充分体现了司法机关以“最严标准”守护校园师生“舌尖上安全”的责任担当，对规范食品生产经营行为，特别是保障校园食品安全具有重要指导和示范意义。

某饮食公司与某中学服务合同纠纷案

【基本案情】

2019 年 6 月 10 日，某饮食公司与某中学签订食堂劳务服务外包项目合同，约定某饮食公司确保食堂运营符合国家食品安全法规，服务期至 2024 年 6 月 9 日。合同履行期间，某饮食公司多次、反复出现严重食品安全问题与管理问题。某中学就厨房环境卫生、部分员工健康证缺漏、食品安全等问题多次发出整改通知，但某饮食公司整改不力，问题未得到根本解决。2021 年 8 月，因某饮食公司未为员工缴纳社保等问题，员工集体辞职，引发管理真空。某中学家委会据此通过决议发起罢餐，并明确指出某饮食公司管理混乱、食品质量低劣。2021 年 8 月 29 日，某中学基于某饮食公司前述违约行为，依据合同约定发出《合同中止通知书》和《合同解除补充通知书》，解除合同并要求清场。某饮食公司认为不符合解约条件，遂起诉请求确认某中学解除合同无效，继续履行合同。

【裁判结果】

法院经审理认为，某饮食公司在履约过程中反复出现食品安全隐患，管理严重失范且经多次整改无效，以致家委会作出决议决定罢餐要求更换食堂管理团队，足以反映师生和家长对学校食堂外包服务的强烈不满。某中学依据合同约定行使解除权，符合法律规定。据此，判决驳回某饮食公司的全部诉讼请求。

【典型意义】

校园食堂外包是当前学校提供餐饮服务的重要方式。外包服务商的责任意识、法律意识、安全意识和严格管理对于保障校园师生“舌尖上的安全”尤为重要。学校发现外包服务商存在食品安全隐患后，有权要求整改，服务商未及时消除隐患，甚至引发罢餐等事件的，学校有权依法解除承包合同。本案中，法院通过支持学校依法解约，防范可能发生的校园食品安全事故，对强化校园食品安全治理具有多重意义：一是确立预防性裁判理念，在校园食堂外包合同纠纷中，当服务商存在持续、严重违约行为且整改无效，已对师生食品安全构成现实风险时，法院应依法支持学校行使解除权，实现对重大食品安全风险的源头预防。二是明晰外包服务商义务与责任，服务商不仅需保障食品安全，还需规范内部管理，达到合同约定的服务质量指标，确保食品安全和服务质量。三是依法保护学生家长参与校园食品安全监督的权利，实现校园食品安全共建共管。

重 要 法 规

中华人民共和国网络安全法

（2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议通过）

第一章 总 则

第 1 条 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第 2 条 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第 3 条 网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

第 4 条 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第 5 条 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第 6 条 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第 7 条 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第 8 条 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第 9 条 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第 10 条　网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第 11 条　建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第 12 条　网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第 13 条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第 14 条　国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第 15 条　任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第 16 条　国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第 17 条　国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第 18 条　国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第 19 条　国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

第 20 条　国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

第 21 条　各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第 22 条　国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章　网络运行安全

第一节　一般规定

第 23 条　国家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，履行下列安全保护义务，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：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第 24 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、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第 25 条　网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第 26 条　网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第 27 条　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；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第 28 条　开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第 29 条　任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等

危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第 30 条　网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第 31 条　国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第 32 条　网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第 33 条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第 34 条　按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

第 35 条　建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第 36 条　除本法第二十一条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第 37 条　关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第 38 条　关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第 39 条　关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第 40 条　关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第 41 条　国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章　网络信息安全

第 42 条　网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

第 43 条　网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第 44 条　网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，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。

第 45 条　个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第 46 条　任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第 47 条　依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第 48 条　任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第 49 条　网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第 50 条　任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第 51 条　网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第 52 条　国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第 53 条　国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门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。

第 54 条　负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第 55 条　国家网信部门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。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第 56 条　网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第 57 条　发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施

和其他必要措施，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。

第 58 条　省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第 59 条　因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第 60 条　因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第 61 条　网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

第 62 条　违反本法第二十二条第一款、第二款和第四十八条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；

拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第 63 条　违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

第 64 条　网络运营者违反本法第二十四条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 65 条　违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第 66 条　违反本法第二十七条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十七条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第 67 条　关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第 68 条　违反本法第四十六条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第 69 条　网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关

业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。

第 70 条　网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）拒绝、阻碍有关部门依法实施的监督检查的；

（二）拒不向公安机关、国家安全机关提供技术支持和协助的。

第 71 条有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

第 72 条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第 73 条　违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

第 74 条　国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；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。

第 75 条　网信部门和有关部门违反本法第三十条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，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。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第 76 条　违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第 77 条　境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章　附　则

第 78 条　本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

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

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第 79 条　存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第 80 条　军事网络的安全保护，由中央军事委员会另行规定。

第 81 条　本法自 2026 年 1 月 1 日起施行。

国家网络安全事件报告管理办法

（2025 年 9 月 11 日　国家互联网信息办公室）

第一条　为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条　在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照本办法的规定进行报告。

第三条　国家网信部门负责统筹协调全国网络安全事件报告管理工作。省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

第四条　网络运营者在发现或获知涉及本单位的网络安全事件时，应当按照《网络安全事件分级指南》（见附件）进行研判，属于较大以上网络安全事件的，按以下程序报告：

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

第五条　网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件。

第六条　鼓励社会组织和个人报告所获悉的较大以上网络安全事件。

第七条　报告网络安全事件时，应当包括下列内容：

（一）涉事单位名称及涉事系统或设施基本情况；

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等；

（三）事态发展趋势及可能造成的进一步影响和危害；

（四）网络安全事件原因初步分析意见；

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等；

（六）拟进一步采取的应对措施以及请求支援事项；

（七）网络安全事件现场保护情况；

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第八条　网络安全事件处置工作结束后，网络运营者应当于 30 日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

第九条　网信部门建设 12387 网络安全事件报告热线电话和网站、邮箱、传真等方式，统一接收网络安全事件报告。

第十条　网络运营者未按照本办法规定报告网络安全事件的，有关主管部门按照有关法律、行政法规的规定进行处罚。

因网络运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

承担网络安全事件报告的部门未按照本办法规定报告网络安全事件的，依据有关法律、行政法规和网络安全工作责任制追究相关单位和人员责任。

第十一条　发生网络安全事件时，网络运营者已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任。

第十二条　本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者。

本办法所指《网络安全事件分级指南》参照《信息安全技术　网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标。

第十三条　涉及国家秘密的网络安全事件报告，按照有关部门规定执行。

第十四条　本办法自 2025 年 11 月 1 日起施行。

最高人民法院关于互联网法院案件管辖的规定

（2025 年 9 月 15 日最高人民法院审判委员会第 1957 次会议通过，自 2025 年 11 月 1 日起施行）

为加强互联网法院建设，优化完善互联网法院的案件管辖，进一步发挥互联网法院司法便民利民、公正高效便捷解纷、强化网络空间依法治理、服务保障数字经济健康发展的功能作用，根据《中华人民共和国民事诉讼法》、《中华人民共和国行政诉讼法》等规定，结合审判工作实际，制定本规定。

第一条　互联网法院集中管辖所在市辖区内应当由基层人民法院受理的下列第一审案件：

（一）网络数据权属、侵权、合同纠纷；（二）网络个人信息保护、隐私权纠纷；（三）网络虚拟财产权属、侵权、合同纠纷；（四）网络不正当竞争纠纷；（五）网络域名权属、侵权、合同纠纷；（六）通过电子商务平台签订或者履行网络购物合同产生的纠纷；（七）签订、履行行为均在网络上完成的网络服务合同纠纷；（八）因行政机关作出网络数据监管、网络个人信息保护监管、网络不正当竞争监管、网络交易管理、网络信息服务管理等行政行为产生的行政纠纷；（九）检察机关提起的网络公益诉讼案件。

符合前款规定的涉外民事案件以及涉香港、澳门特别行政区和台湾地区的民事案件，由互联网法院管辖。

经最高人民法院批准，相关高级人民法院可以指定互联网法院管辖其他特定类型的网络民事、行政案件。

第二条　对于本规定第一条确定的合同及其他财产权益民事纠纷，当事人可以依法协议约定与争议有实际联系地点的互联网法院管辖。当事人之间采取格式条款形式约定案件由互联网法院管辖的，应当符合法律及司法解释关于格式条款的规定。

第三条　当事人对互联网法院作出的判决、裁定提起上诉的案件，由互联网法院所在地的中级人民法院审理。所在地设有多个中级人民法院的，由高级人民法院指定的中级人民法院审理。上诉案件属于专门人民法院管辖范围的，由相应的专门人民法院审理。

第四条　本规定自 2025 年 11 月 1 日起施行。本规定施行前已经受理的案件由原受理人民法院继续审理。

此前发布的司法解释与本规定不一致的，以本规定为准。

电子印章管理办法

第一章　总则

第一条　为了加强电子印章规范管理，推动电子印章普遍应用，服务政务活动和经济社会数字化发展，根据《中华人民共和国电子签名法》、《中华人民共和国密码法》、《中华人民共和国网络安全法》、《中华人民共和国数据安全法》以及印章管理有关法律法规，制定本办法。

第二条　本办法所称电子印章，是指基于密码技术和相关数字技术表征印章的特定格式数据，用于实现电子文件的可靠电子签名。

电子印章包含印章图像数据、印章名称、印章所有者信息、电子签名认证证书以及与其关联的电子签名制作数据等。

第三条　本办法适用于行政机关、企业事业单位、社会组织以及其他依法成立的组织〔以下统称单位（组织）〕的法定名称章，以法定名称冠名的内设机构章、分支机构章、业务专用章，以及用于单位（组织）事务办理的个人名章等电子印章的管理和应用活动。

第四条　电子印章管理工作遵循统筹推进、分级管理、规范标准、安全可控的原则。

第五条　符合本办法规定的电子印章与实物印章具有同等法律效力。除法律、行政法规明确不适用的情形外，经电子签章的电子文件与加盖实物印章的纸质文件具有同等效力。

第二章　管理和服务主体

第六条　国家密码管理局负责电子印章有关密码管理工作，对电子印章相关的电子政务电子认证服务实施监督管理，推动电子印章标准化工作，促进电子印章在政务活动中的互信互认。

国家密码管理局会同有关部门统筹协调和推进全国电子印章的规范管理和推广应用。

第七条　国务院办公厅负责依托全国一体化政务服务平台推动政务服务、公共服务以及相关社会化服务领域电子印章的互信互认。

第八条　工业和信息化部负责对电子印章相关的电子认证服务实施监督管理。

第九条　公安机关负责依法打击涉及电子印章的违法犯罪行为。

第十条　省、自治区、直辖市密码管理部门负责本行政区域内电

子印章有关密码管理工作，对电子印章相关的电子政务电子认证服务实施监督管理，推动电子印章标准化工作，促进电子印章在政务活动中的互信互认。

第十一条　各地区各部门应当统筹加强本地区本部门（本系统）电子印章的规范管理和推广应用，促进电子印章互信互认。

（一）各省（自治区、直辖市）、国务院各部门应当参照印章管理有关法律法规明确电子印章制发部门，负责本地区本部门（本系统）电子印章申请和注销的管理。（二）各省（自治区、直辖市）应当明确电子印章制作管理单位，负责本地区电子印章的制作、备案等工作。国务院各部门根据职责范围和实际需要明确电子印章制作管理单位，负责本部门（本系统）电子印章的制作、备案等工作。

第十二条　电子印章涉及的电子政务电子认证服务，应当由依法设立的电子政务电子认证服务机构提供。电子印章涉及的电子认证服务，应当由依法设立的电子认证服务机构提供。

第三章　制作、备案与注销管理

第十三条　电子印章制发部门应当参照印章管理有关法律法规，明确申请电子印章的程序和要求。

企业、社会组织等申请电子印章的程序可以结合实际适当简化。

第十四条　电子印章制作管理单位应当明确电子印章制作程序、材料等具体要求。单位（组织）应当按照要求提交真实、合法、有效的制作材料，由电子印章制作管理单位进行核查。

相关材料应当包含：

（一）电子印章申请通过的相关证明材料；（二）单位（组织）的设立批准文件或者设立登记证件；（三）制作电子印章的相关数据和信息；（四）电子印章制作管理单位规定提交的其他材料。

鼓励电子印章制作管理单位优先通过数据共享方式获取上述相关材料。

第十五条　鼓励和支持电子印章制作系统与提供电子签章、电子签章验证等功能的信息系统独立部署。电子印章制作系统存在条块交叉的，应当统筹协调、集约建设。

第十六条　电子印章制作应当符合以下要求：

（一）电子印章的电子签名认证证书应当合法有效，由依法设立的电子政务电子认证服务机构或者电子认证服务机构签发，电子印章有效期的截止时间不超过电子印章所有者电子签名认证证书有效期的截止

时间；（二）电子印章的数据格式、生成流程和应用接口应当符合国家有关标准规范；（三）电子印章的图像规格、式样等图像数据应当与印章管理有关法律法规明确的印模规制保持一致，可以根据需要附加电子印章相关标注字样。无对应实物印章的，电子印章图像数据可以参照相近实物印章的印模规制。

第十七条　电子印章制作完成后，电子印章相关信息应当由电子印章制作管理单位进行备案。发生电子印章停用、恢复等状态变更情形的，电子印章所有者或者相关单位应当及时向电子印章制作管理单位进行备案。

电子印章制作管理单位应当提供电子印章状态信息查询服务。

第十八条　因电子印章有效期到期、电子印章载体损坏或者遗失、电子签名制作数据失密等情形需要重新制作电子印章的，电子印章所有者应当向电子印章制作管理单位提出重新制作。重新制作流程可以结合实际适当简化。

第十九条　电子印章所有者发生更名、解散、撤销、被吊销、破产、分立、合并等情形，应当注销电子印章。电子印章所有者应当按照要求及时向电子印章制发部门提出注销电子印章，电子印章制作管理单位根据电子印章制发部门的处理意见，对需要注销的电子印章进行注销备案。

电子印章所有者应当注销电子印章但未注销或者无法及时提出注销电子印章的，由电子印章制发部门提出注销处理意见，电子印章制作管理单位对需要注销的电子印章进行注销备案。

电子印章所有者根据需要可以主动提出注销电子印章。

第二十条　电子印章制作管理单位可以自行或者委托相关单位具体实施电子印章的制作、备案等工作，其中涉及的密码产品、服务应当符合密码检测认证有关要求。电子印章制作管理单位应当对受委托单位所承担的电子印章制作、备案等工作加强监督。

电子印章制作、备案的操作记录、操作结果应当由电子印章制作管理单位妥善保管、长期保存。

第四章　使用管理

第二十一条　电子印章使用管理遵循“谁所有、谁控制，谁签章、谁负责”的原则。电子印章所有者应当制定有关规章制度，妥善保管和规范使用电子印章。

第二十二条　电子签章应当使用有效的电子印章，遵照国家有关法律法规和标准规范，保证电子签章数据的真实性、完整性和不可否认性。电子签章过程信息应当被记录并保存，实现电子签章行为可追溯、可定责。

第二十三条　电子签章验证应当按照国家有关标准规范核验电子签章数据的真实性、完整性和不可否认性，并核验电子印章在电子签章时的有效性。

第二十四条　经电子签章的电子文件归档时，应当符合电子档案管理有关规定和标准规范。

第五章　互信互认

第二十五条　国家推动电子印章跨地区跨部门互信互认支撑能力建设，规范电子印章编码，促进电子印章状态信息及相关电子签名认证证书链信息的共享和使用。

各地区各部门应当结合实际，加强本地区本部门（本系统）电子印章互信互认支撑能力建设。

第二十六条　国家密码管理局会同有关部门积极推动电子印章互信互认标准规范建设，促进电子印章制作、备案、使用等环节的标准化。

第二十七条　行政机关以及履行社会管理和公共服务职能的企业事业单位、社会组织在业务活动中需要使用电子印章时，其业务信息系统应当支持符合本办法规定的电子印章接入使用，法律、行政法规另有规定的除外。

经电子签章的电子文件应当实现跨层级跨地域跨系统跨部门跨业务互通互认。

第六章　安全管理

第二十八条　电子印章管理全过程应当建立完善的信息保护制度，采取必要措施确保电子印章相关信息的安全，并对收集的单位（组织）和个人的信息严格保密，防止未经授权的访问以及信息泄露、篡改或者毁损、丢失。

第二十九条　电子印章相关信息系统的建设、使用和运行维护应当符合国家密码管理、网络安全、数据安全等相关法律法规和标准规范。

涉及国家秘密信息的电子印章相关信息系统的建设、使用和运行维护，还应当按照国家保密管理有关规定执行。

第七章　违法违规责任

第三十条　受委托承担电子印章制作、备案等工作的单位，未按照有关法律法规和标准规范制作电子印章，未按照规定履行安全管理义务，或者有其他违法行为的，由有关部门责令限期改正，并由电子印章制作管理单位将违法违规制作的电子印章标识为无效；逾期未改正的，由有关部门依法依规追究责任。

电子政务电子认证服务或者电子认证服务存在违法行为，影响相关电子印章有效性的，由电子印章制作管理单位将涉及的相关电子印章标识为无效。

第三十一条　电子印章所有者违反本办法规定的，依法依规承担相应责任。

第三十二条　伪造、变造、冒用、盗用电子印章的，依法依规承担相应责任。

第三十三条　依照本办法对电子印章相关活动负有监管职责的有关部门工作人员，不依法依规履行责任、失职渎职的，依法依规追究有关人员的责任；涉嫌犯罪的，移送有关机关处理。

第八章　附则

第三十四条　本办法中下列用语的含义：

（一）电子印章所有者，是指对电子印章拥有所有权的单位（组织）或者个人。电子印章的电子签名制作数据属于电子印章所有者专有。

（二）电子签章，是指使用电子印章签署电子文件的过程，所形成的结果数据为电子签章数据。

（三）电子印章制作系统，是指主要提供电子印章制作及相关管理功能的信息系统。

第三十五条　仅用于单位（组织）内部业务的电子印章，可以参照本办法有关规定自行组织制作和管理。

第三十六条　行政机关以外的其他国家机关可以参照本办法规范本部门（本系统）电子印章管理和应用活动。

第三十七条　法律法规以及国家有关规定对涉密领域电子印章管理有特别规定的，依照其规定。

第三十八条　本办法自印发之日起施行。

新颁布或修订的主要法律规范目录

1、中华人民共和国城市居民委员会组织法

（2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议修订）

2、中华人民共和国海商法

（2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议修订）

3、中华人民共和国网络安全法

（根据 2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议《全国人民代表大会常务委员会关于修改＜中华人民共和国网络安全法＞的决定》修正）

4、中华人民共和国环境保护税法

（根据 2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议《全国人民代表大会常务委员会关于修改＜中华人民共和国环境保护税法＞的决定》第二次修正）

5、中华人民共和国村民委员会组织法

（根据 2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议《关于修改〈中华人民共和国村民委员会组织法〉的决定》第二次修正）

6、中华人民共和国食品安全法

（根据 2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议《关于修改＜中华人民共和国食品安全法＞的决定》第三次修正）

7、中华人民共和国法治宣传教育法

（2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议通过）

8、中华人民共和国仲裁法

（2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议修订）

9、中华人民共和国国家公园法

（2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议通过）

10、中华人民共和国突发公共卫生事件应对法

（2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议通过）

11、中华人民共和国原子能法

（2025 年 9 月 12 日第十四届全国人民代表大会常务委员会第十七次会议通过）

12、最高人民法院关于互联网法院案件管辖的规定

（2025 年 9 月 15 日最高人民法院审判委员会第 1957 次会议通过，自 2025 年 11 月 1 日起施行 法释〔2025〕14 号）