附件 1：

南通市司法局信息网络安全管理工作方案

第一章　总　则

第一条　为规范南通市司法局信息化及计算机网络安全管理，促进信息化建设，提高工作效率，确保信息化网络计算机设备安全、有效运行，特制定本制度。

第二条　南通市司法局信息化及计算机网络管理工作在市局党组的统一领导下，由南通市司法局网络安全和信息化领导小组所有成员负责具体组织实施。

第三条　本单位计算机信息网络安全管理工作实行“一把手”负责制。

第四条　本制度所称计算机信息安全网络管理工作包 括信息化网络及设备管理、安全保密管理、计算机病毒防治、资料管理、培训等内容。

第二章　信息化网络及设备管理

第五条　信息化网络及设备按个人分配使用。分配到个人的设备由信息化部门的工作人员负责，单位应指定一名熟悉计算机技术的人员负责日常管理和维护工作。

第六条　凡使用信息化网络及设备的工作人员应自觉遵守

相关法律法规和制度规定。对违反规定使信息化网络及设备不能正常工作和造成重大事故者，追究其相应责任，后果严重的，依法追究法律责任。

第七条 严禁在信息化设备上安装与工作无关的、未经广泛验证为安全的软件程序。严禁带电拔插计算机内部配件。移动非便携式信息网络设备应断电后进行。离开工作场所前，须关闭计算机，切断电源。如有特殊情况不能关闭的，须征得本部门负责人同意。

第八条 非指定的技术人员不得擅自打开信息化网络设备外壳，进行任何配置和检测。不得擅自将信息网络设备（包括报废设备）的配件私自拆卸，移植到其它设备。

第九条 未经单位负责人批准，任何人不得随意更换信息化网络设备，不得随意外借、处置信息网络设备。外部人员如需使用本单位的信息网络设备，需经本单位信息化部门同意，并在现场监督的情况下进行。

第十条 对计算机进行硬盘格式化和删除操作系统文件，须事先做好数据备份工作，并由本单位信息化管理员进行操作。

第十一条 各部门信息化网络设备的使用人、保管人、责任人等情况的变更，应及时报装备财务部门登记备案。

第十二条 重要的信息化网络设备，由装备财务部门集中统一管理。如需要使用时，应办理相关借用手续。

第十三条 为防止计算机病毒造成严重后果，对外来移动存

储介质（软盘、光盘、优盘、移动硬盘等）要严格管理，原则上不允许外来移动存储介质在内部专网计算机上使用。确因工作需要使用的，事先必须进行防毒处理，经技术人员证实无病毒感染后，方可使用。

第十四条 本单位应定期对本单位信息化网络设备进行系统维护及必要的数据备份，并安装指定的杀毒软件，进行定期杀毒、系统漏洞修补、杀毒软件升级。

第十五条 信息化网络设备报废或调拨时，须进行必要的清理工作，防止资料泄密。

第十六条 为保障信息化网络设备安全、稳定、持续运行，发挥最优性能，设备必须按照技术人员制定的方案和要求进行统一配置设备的使用者不得拒绝，并不得随意更改设备已配置好的参数。

第十七条 网络使用与管理应遵循以下原则。

1．每位工作人员都有义务维护工作用计算机网络的正常运行，并严格遵照有关的规定入网。

2．在工作用网络上只允许进行与业务工作有关的操作，不得进行非法操作。一经发现，将依照有关规定进行处理。

3．不得在工作用网络上传播计算机病毒，造成损失的，将依照国家法律，移交有关部门处理。

4．不得通过工作用网络系统进行营利性的商业行为及散发任何的垃圾邮件。

5．要严格遵守国家关于网络管理的相应法律，不得在网上传播和散布反动、淫秽信息，也不得散布攻击他人的言论。

6．任何人不得对工作用网络设施和信息文件有意破坏和攻击，对于采取破坏手段，无论是否造成不良后果的，追究其个人及所在单位领导责任。

7．工作用涉密网络与国际互联网要完全物理隔离，严禁把工作用涉密网络以任何方式连接到国际互联网上。

8．严禁将涉密网络延伸至任何无线网络系统。

9．个人的入网口令应注意保密，防止其他用户侵入网络设备，保证数据资料安全。

第十八条　信息网络设备故障处理应遵循以下原则。

1．信息网络设备发生故障后，由本单位信息化管理人员进行排除，如无法排除，由单位技术主管人员协同处理。需要请专业公司维修的，按相关程序进行报修。

2．信息网络设备需要更换配件（耗材），经单位技术主管人员确认，并按相关规定程序报批后进行。

3．信息网络设备要报废的，按单位固定资产报废的程序进行。

第三章　安全保密管理

第十九条　网络安全工作领导小组负责对本单位计算机信息系统安全和保密工作进行指导和检查。单位相关人员要密切配

合，共同做好计算机信息系统安全和保密工作。

第二十条 加强保密意识教育，提高工作人员保密观念，增强防范意识，自觉执行保密规定。

第二十一条 单位应与重点岗位的计算机使用人员签订安全保密责任书，明确安全和保密要求与责任。

第二十二条 计算机使用人员离岗离职，有关部门应当即时取消其计算机信息系统访问授权，收回计算机、移动存储设备等相关物品。

第二十三条 单位要加强内部计算机信息系统安全和保密管理情况的监督，定期开展自我检查、自我评估，发现问题及时纠正。

第二十四条 计算机信息系统使用管理人员违反本规定，情节较轻的，由本单位予以批评教育；情节严重，造成 安全和泄密隐患的，按有关规定处理。

第二十五条 违反本规定泄露国家秘密的，按照有关规定给予直接责任人和有关领导行政或者党纪处分；构成犯罪的，依法追究刑事责任。

第二十六条 本单位要结合实际，制定完善本单位计算机信息系统安全和保密管理的具体办法。

第二十七条 涉密计算机或其它涉密终端一律禁止连接国际互联网。如有特殊需求，必须事先提出申请报主管领导批准后方可实施，并由技术主管人员全程介入，在相关工作完成后立即

切断与外部网络连接。

第二十八条 坚持“谁上网，谁负责”的原则，本单位信息化部门负责审查本单位人员计算机上网资格。

第二十九条 国际互联网须与涉密计算机实行物理隔离。

第三十条 在与国际互联网相连接的信息设备上不得存储、处理和传输任何涉密信息。

第三十一条 涉密计算机维护管理应遵循以下原则。

1．涉密计算机系统进行维护检修时，须保证所存储的涉密信息不被泄露，对涉密信息应采取涉密信息转存、删除、异地转移存储媒介等安全保密措施。无法采取上述措施时，单位技术主管人员须在维修现场监督，并对维修人员、维修对象、维修内容、维修前后情况做好详细记录。

2．应将本单位设备的故障现象、故障原因、扩充情况记录在设备的维修档案记录本上。

3．凡需外送修理的涉密设备，必须经主管领导批准，并将涉密信息进行不可恢复性删除处理后方可实施。

4．本单位应指定专人负责各涉密单位计算机软件的安装和设备的维护维修工作，严禁擅自安装计算机软件和擅自拆卸计算机设备。

5．涉密计算机的报废须由主管领导同意，专人监督、专人负责定点销毁。

第四章　计算机病毒防治

第三十二条　涉密计算机必须安装经过国家安全保密部门许可的查、杀病毒软件。

第三十三条　每周定期升级和查杀计算机病毒软件的病毒样本，确保查杀病毒软件始终处于最新版本。

第三十四条　严禁涉密计算机在线升级防病毒软件病毒库。采用离线方式升级的，要对其升级包来源进行登记。

第三十五条　每周对涉密计算机进行一次病毒查杀。

第三十六条　涉密计算机应限制信息入口，如软盘、光盘、优盘、移动硬盘等的使用。

第三十七条　对必须使用的外来介质（磁盘、光盘，优盘、移动硬盘等），必须先进行计算机病毒的查杀处理，然后才可使用。

第三十八条　对于因未经许可而擅自使用外来介质导致严重后果的，要严格追究相关人员的责任。

第五章　资料管理

第三十九条　电子文件资料(指在计算机系统中生成、存储、处理的机密、秘密和内部的文件、图纸、程序、数据、声像资料等）管理应遵循以下原则。

1．涉密电子文件资料须在具有安全保障措施的涉密计算机上处理和存放。

2．电子文件的密级按其所属项目的最高密级界定，其生成者应按密级界定要求标定其密级，并将文件存储在相应的目录下。

3．电子文件要有密级标识，电子文件的密级标识不能与文件的正文分离，一般标注于正文前面。

4．电子文件必须定期、完整、真实、准确地存储到不可更改的介质上，并集中保存。

5．单位自用信息资料要定期做好备份，备份介质必须标明备份日期、备份内容以及相应密级，严格控制知悉此备份的人数，做好登记后进保密柜保存。

6．单位要对备份电子文件进行规范的登记管理。备份可采用磁盘、光盘、移动硬盘、优盘等存储介质。

7．备份文件和资料保管地点应有防火、防热、防潮、防尘、防磁、防盗设施，并进行异地备份。

第四十条 涉密人员在其它场所上国际互联网时，要提高保密意识，不得在聊天室、电子公告系统、网络新闻上发布、谈论和传播国家秘密信息。

第四十一条 禁止将涉密计算机或其它涉密终端擅自联接国际互联网，禁止将非涉密计算机或其它非涉密终端联入涉密网络。

第四十二条 移动存储设备不得在涉密信息系统和非涉密信息系统间交叉使用，涉密移动存储设备不得在非涉密信息系统中使用。

第四十三条 保密级别在秘密以下的材料可通过互联网以电子信箱、FTP 等方式传递和报送，严禁保密级别在秘密以上的材料通过互联网以任何方式传递和报送。在内部专网上传输保密级别在秘密以上的电子材料，也必须先加密后传输。

第四十四条 严禁使用含有无线网卡、无线鼠标、无线键盘等具有无线互联功能的设备处理涉密信息。

第六章 培 训

第四十五条 本单位要重视信息化网络和计算机技术培训工作，积极派员参加本系统组织的各种计算机培训，努力培养专业技术骨干人才，提高单位网络安全工作水平。

附件 2：

南通市司法局网络安全工作责任制实施细则

第一条 为进一步加强网络安全工作，明确和落实党委（党组）领导班子、领导干部网络安全责任，根据《中华人民共和国网络安全法》《中国共产党问责条例》、中共中央办公厅《党委（党组）网络安全工作责任制实施办法》、省委办公厅《党委（党组）网络安全工作责任制实施细则》、市委办公室《党委（党组）网络安全工作责任制实施细则》等法律法规和政策规定，制定本实施细则。

第二条 本实施细则适用于本部门本行业党委（党组）领导班子、领导干部。

事业单位、人民团体的党委（党组）领导班子、领导干部参照执行。

第三条 网络安全工作事关国家安全、政权安全和经济社会发展。按照谁主管谁负责、属地管理的原则，党委（党组）对本部门本行业网络安全工作负主体责任，领导班子主要责任人是第一负责人，主管网络安全的领导班子成员是直接责任人。

第四条 党委（党组）主要承担的网络安全责任是：

1．认真贯彻落实党中央、习近平总书记和省委市委关于网络安全工作的重要指示精神和决策部署，贯彻落实网络安全法律法规、标准规范和政策要求，明确本部门网络安全的主要目标、

基本要求、工作任务、保障措施；

2．建立和落实网络安全责任制，把网络安全工作列入重要议事日程，明确主管网络安全的领导班子成员、网络安全领导机构和工作机构，加大人才、财力、物力的支持和保障力度；

3.统一组织领导本部门网络安全保护和重大事件处置工作，研究解决重要问题；

4．采取有效措施，为公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动提供支持和保障；

5．推动网络安全宣传教育培训常态化，提升全体网络安全意识，支持多方式多层次网络安全人才培养；

6．加大网络安全技术产业发展扶持力度，推广应用安全可信的网络安全产品、密码产品和服务，加大国产化推进力度。

第五条 市司法局对本行业本领域的网络安全负指导监管责任。责任主要有：

1．编制本行业本领域网络安全工作规划，指导督促行业领域内关键信息基础设施运营者加强安全管理和防护，保障网络安全和数据安全；

2．制定修订本行业本领域网络安全事件应急预案，建立健全行业领域应急专家组和技术支撑队伍，每年定期组织开展应急演练；

3．依法开展本行业本领域网络安全检查，组织开展技术检测和风险评估，依法处置网络安全事件，并及时将情况通报网络

和信息系统所在地区网络安全和信息化领导小组。

第六条 网络安全和信息化领导小组应当加强统一领导，重点做好以下工作：

1．统筹协调组织本地区本部门网络安全应急、安全检查、安全审查、监测预警、通报处置，宣传教育等工作，重点做好关键信息基础设施和重要数据资源保护工作，开展网络安全检查、处置网络安全事件时，涉及重要行业的，应当会同行业主管监管部门进行；

2．加强和规范本部门网络安全信息汇集、分析和研判工作，要求有关单位和机构及时报告网络安全信息，推动网络全信息共享共用；

3．统筹推进本部门网络安全监测预警、态势感知、应急指挥、新技术新应用安全监管等保障和监管能力建设。

第七条 各级网络安全和信息化领导小组每年向上级网络安全和信息化领导小组报告本地区本部门上一年度网络安全工作情况，并及时报告网络安全重大事项，主要包括：

1．上级网络安全和信息化领导小组交办和督办事项执行情况；

2．出台涉及网络安全的重要政策和制度措施，以及开展重要执法和宣传教育活动等情况；

3．网络安全重点工作、重点项目、重大工程进展情况；

4．重大网络安全事件及处置情况；

5．其他应当报告的事项。

第八条 党委（党组）违反或未能正确履行本实施细则所列职责，按照有关规定追究相关责任。有下列情形之一的，各级党委（党组）应当逐级倒查，追究当事人、网络安全负责人直至主要负责人责任。协调监管不力的，还应当追究综合协调或监管部门负责人责任。

1．党政机关门户网站、重点新闻网站、大型网络平台被攻击篡改，导致反动言论或谣言等违法有害信息大面积扩散，且没有及时报告和组织处置的；

2．党政机关门户网站或重点新闻网站受到攻击后没有及时组织处置，且瘫痪6小时以后的；

3．发生国家秘密泄露、大面积个人信息泄露或大量地理人口、资源等国家基础数据泄露的；

4．关键信息基础设施遭受网络攻击，没有及时处置导致大面积影响人民群众工作、生活，或者造成重大经济损失，或者造成严重不良社会影响的；

5．封锁、瞒报网络安全事件情况，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的；

6．阻碍公安机关、国家安全机关依法维护国家安全、侦查犯罪以及防范、调查恐怖活动，或者拒不提供支持和保障的；

7．重大活动、重要时期网络安全保障不力并造成严重后果

的；

8. 发生其他严重危害网络安全行为的。

第九条 实施责任追究应当实事求是，分清集体责任和个人责任。追究集体责任时，领导班子主要负责人和主管网络安全的领导班子成员承担主要领导责任，参与相关工作决策的领导班子其他成员承担重要领导责任。对领导班子、领导干部进行问责，应当由有管理权限的党组织依据有关规定实施。

第十条 各级党委（党组）应当建立网络安全责任制检查考核制度，完善健全考核机制，明确考核内容、方法、程序，将网络安全工作责任落实情况作为巡察监督重要内容，纳入本部门年度目标责任考核指标，作为对领导班子和有关领导干部年度考核评价的重要内容。

第十一条 市司法局网络安全和信息化领导小组办公室会同市有关部门，制定我局网络安全工作责任制考核办法和评价指标体系，组织开展本部门网络安全督查考核工作，按照国家和省市有关规定对成绩突出的予以褒奖。

第十二条 网络意识形态工作责任制按照《市司法局网络安全工作责任制实施细则》执行。涉密网络按照有关规定执行。

第十三条 本实施细则由中共南通市司法局党组负责解释，具体解释工作由市司法局办公室商市司法局网络安全和信息化领导小组办公室负责。

第十四条 本实施细则自印发之日起施行。

附件 3：

南通市司法局网络与信息安全事件应急预案

一、总则

（一）目的

为切实加强我局网络运行与信息安全，做好应对网络与信息安全突发公共事件的应急处理工作，进一步提高预防和控制网络突发公共事件的能力和水平，减轻或消除网络突发公共事件的危害和影响，做好网上舆论管理和信息安全保障工作，确保网络运行安全与信息安全，结合我局工作实际，制定本预案。

（二）原则

1．积极防御，综合防范。立足安全防护，加强预警，抓好预防、监控、应急处理、应急保障和打击犯罪等环节，在管理、技术、人才等方面，采取各种措施，充分发挥各方作用，共同构筑我局网络与信息安全保障体系。

2．明确责任，分级负责按照“谁主管谁负责，谁运维谁负责”的原则，分级分类建立和完善安全责任制度、协调管理机制和联动工作机制。

3．科学决策，快速反应。加强技术储备，规范应急处置措施和操作流程，网络与信息安全突发公共事件发生时，要快速反应，及时获取准确信息，跟踪研判，及时报告，果断决策，迅速处理，最大限度地减少危害和影响。

（三）适用范围

本预案适用于我局发生的网络与信息安全突发公共事件和可能导致网络与信息安全突发公共事件的处置工作。

二、组织体系

成立网络与信息安全应急领导小组和应急工作小组

（一）应急领导小组

组　长：朱志强

副组长：肖建源

成　员：市局各处室第一负责人

（二）应急领导小组职责

统一领导网络与信息安全的应急工作，全面负责信息网络可能出现的各种突发公共事件处置工作。发生网络与信息安全突发公共事件时，启动本预案，组织应急处置。

（三）应急工作小组

组　长：居乔年

成　员：曹清媛、张晶韡

（四）应急工作小组职责

1. 负责和处理应急领导小组的日常工作，执行、检查、督促应急领导小组决定的工作事项。

2. 组织开展网络与信息安全的自查自纠，排查安全隐患，发现问题立即整改，每天检查网络运行状态。

3. 建立网站舆情监控机制。一旦发现负面信息或异常舆情，以最快的时间屏蔽负面信息，必要时进一步关闭服务器，切断网

络连接。尽快向应急领导小组组长汇报，组织技术力量和相关人员查找原因，提出解决办法。

4. 收集有可能导致网络与信息安全突发公共事件的潜在信息，分析情况，预判问题，及时向应急领导小组提出预处理意见。对可能演变为网络与信息安全突发公共事件的，尽快向应急领导小组提出启动本预案的建议。

三、预防预警

（一）信息监测与报告

1. 进一步完善网络与信息安全突发公共事件监测、预测和预警制度。落实工作责任制，按照“早发现、早报告、早处置”的原则，加强对各类网络与信息安全突发公共事件和可能引起突发网络与信息安全突发公共事件的有关信息的收集、分析、判断和持续监测。当检查到有网络与信息安全突发公共事件发生时，立即向应急领导小组报告（初次报告最迟不得超过半小时）。报告内容主要包括信息来源、影响范围、事件性质、事件发展趋势和采取的措施建议等。

2. 发现下列情况应及时向应急领导小组报告：利用网络从事违法犯罪活动；网络或信息系统通信和资源使用异常；网络或信息系统瘫痪，应用服务中断或数据篡改、丢失；网络恐怖活动的嫌疑和预警信息；其他影响网络与信息安全的信息。

（二）预警处理与发布

1. 对可能发生或已经发生的网络与信息安全突发公共事件，立即采取措施，制止事件的延续、蔓延，并在 1 小时内进行风

险评估，必要时启动相应预案，同时向应急领导小组报告。

2．应急领导小组接到报告后，对可能发生或已经发生的网络与信息安全突发公共事件，迅速召开应急领导小组会议，启动本预案，研究确定处置意见。

3．对需要向上级相关部门通报的，要及时通报，并争取支援。

四、应急响应

（一）先期处置

当我局网络上出现不良信息时，监控人员应立即采取措施控制事态，立即屏蔽信息；能删改的信息，立即删改；无法删改的信息，应立刻关闭服务器，并详细备案，同时向应急工作小组组长报告。处理后，应对网络进行查病毒、查木马，检测是否受到攻击，排查事件原因。

应急工作小组组长接到报告后，应加强与有关方面的联系，掌握最新发展动态，追查原因。对发生重大和有可能演变为重大的网络与信息安全突发公共事件，要立即报告应急领导小组，并做好启动本预案的各项准备工作；应急领导小组在接到报告后，要根据网络与信息安全突发公共事件发展态势，视情况决定是否赶赴现场指挥，组织派遣应急支援力量。

（二）应急指挥

本预案启动后，应急领导小组要抓紧收集相关信息，掌握现场处置工作状态，分析事件发展态势，研究提出处置方案，统一指挥网络与信息应急处置工作。需要成立现场指挥部的，应立即

在现场开设指挥部，现场指挥部要根据事件性质组建各类应急工作小组，开展应急处置工作。必要时，向相关部门申请应急支援。

（三）信息处理

应急工作小组应对事件进行动态监测、评估，不得隐瞒、缓报、谎报。要做好信息分析、报告和发布工作，及时提供事件动态信息给应急领导小组研究决策。应组织专家和有关技术人员研判各类信息，研究提出处置措施，完善应急处置计划方案。

五、后期处置

（一）善后处理

应急处置工作结束后，应急工作小组要迅速采取措施，抓紧组织抢修受损的基础设施，减少损失，尽快恢复正常工作。统计各种数据，查明原因，对事件造成的损失和影响以及恢复重建所需的时间、费用等进行分析评估，认真制定恢复重建计划，并迅速组织实施。最后，要将善后处置的有关情况报应急领导小组。

（二）调查评估

应急处置工作结束后，应急工作小组应立即组织有关人员和专家组成事件调查组，对事件发生及其处置过程进行全面的调查，查清事件发生的原因及损失情况，总结经验教训，写出调查评估报告，报应急领导小组。

六、保障措施

（一）应急装备保障

对于重要网络与信息系统，在建设系统时应事先预留一定的应急设备，建立信息网络硬件、软件、应急救援设备等应急物资

库。在网络与信息安全突发公共事件发生时，报应急领导小组同意后，由应急工作小组负责统一调用。

（二）数据保障

重要信息系统均应建立容灾备份系统和相关工作机制，保证重要数据在遭到破坏后，可紧急恢复。各容灾备份系统应具有一定的兼容性，在特殊情况下各系统间可互为备份。

七、监督管理

（一）要充分利用各种传播媒介及有效的形式，加强网络与信息安全突发公共事件应急和处置的有关法律法规和政策的宣传。

（二）建立应急预案定期演练制度。通过演练，发现应急工作体系和工作机制存在的问题，不断完善应急预案，提高应急处置能力。

（三）对在网络与信息安全突发公共事件应急处置中作出突出贡献的集体和个人，给予表彰奖励；

对在网络与信息安全突发公共事件预防和应急处置中有玩忽职守、失职、渎职等行为，依法依规追究责任。

八、附则

本预案自印发之日起实施。