

宁波市大数据发展管理局文件

甬数管〔2021〕13号

宁波市大数据发展管理局 关于印发宁波市大数据发展管理局网络 数据安全管理的实施细则的通知

局机关各处、市大数据管理服务中心、市智慧城市规划标准发展研究院,各有关单位:

《宁波市大数据发展管理局网络数据安全管理的实施细则》已经局党组会议审议通过,现印发给你们,请认真组织实施。



宁波市大数据发展管理局 网络数据安全实施细则

第一条 为落实《中华人民共和国网络安全法》《中华人民共和国数据安全法》《浙江省公共数据和电子政务管理办法》《浙江省公共数据开放与安全暂行管理办法》《宁波市公共数据安全暂行管理办法》《宁波市公共数据管理办法》等法律法规规定，加强市大数据局网络数据安全管理工作，保障网络数据安全，制定本细则。

第二条 市大数据局及内设各处室和下属单位（以下简称各处室）负责的网络数据安全管理工作，适用本细则。

本细则所称网络数据安全管理工作，包括市大数据局及各处室负责建设、运营、维护、使用、管理的网络/物联网、数据平台/政务云平台、信息系统/应用系统和数据采集、归集、存储、使用、加工、传输、共享、开放等数据治理工作的安全监管。

第三条 市大数据局成立由主要领导任组长的局网络信息安全工作领导小组，全面落实网络信息安全主体责任，定期会商网络数据安全管理工作。领导小组下设办公室（设在数字基础设施和安全处），负责局网络信息安全日常管理，牵头拟订并组织实施网络数据安全总体应急预案和年度工作方案，组织开展应急演练，组织或协同网信、公安等部门开展网络信息安全检查，开

展服务商网络安全背景审查，组织网络数据安全培训，组织开展网络数据安全重保活动。

各处室负责落实各自职责相应的网络数据安全工作职责，建立健全网络数据安全管理工作机制，将安全责任具体落实到人，组织制定各系统应急预案和操作手册，组织相关应急演练，并形成相应的记录文档，落实网络数据安全相关工作。

第四条 所有网络信息系统必须严格落实等级保护制度，按照同步规划、同步建设、同步使用的“三同步”原则，及时定级备案和测评整改。等保三级以上信息系统落实商用密码应用安全性评估。

各处室应针对应用系统的安全需求，制定有效的安全措施，并对安全措施的有效性进行必要的评估、验证。

第五条 各处室应当与各第三方服务团队签订网络安全、数据安全和保密等协议，明确责任边界和违约责任。

网络数据安全管理工作责任不随服务外包而转移，无论数据、系统和服务是位于独立设备、云平台还是在外部服务商，各处室始终是网络数据安全的最终责任人。

第六条 各处室发现网络使用管理或数据处理存在安全隐患、网络威胁和安全事故时，应当及时告知领导小组办公室或直接报告领导小组，同时按规定报告网信或有关部门和告知用户，并采取措施加以预防、制止或处置。在发生特殊的网络信息安全突发应急事件时，可先采取包括停止服务在内的紧急措施，以避

免信息安全事件的进一步扩大。当安全隐患、网络威胁和安全事故消除后，应及时恢复正常使用。

对网络数据安全风险处置涉及有关单位和个人的，领导小组或办公室可以按有关规定对有关单位和个人进行约谈，并要求进行整改，消除隐患。

第七条 所有使用人不得利用本单位网络从事违反国家法律法规和单位有关规章制度的活动，不得在互联网上发表和散布错误和非法言论，不得登录非法和违规网站。

不得以任何手段破坏、阻碍、修改或窃取单位网络正常传输的数据，不得对单位所有的各种设备、软件和系统进行攻击和非法侵入。

不得在终端和设备上运行非法程序和恶意软件，访问未授权地址和非法地址。

第八条 各处室管理的各种终端、设备、软件和系统原则上通过市级政务外网的统一互联网出口连接国际互联网，未经许可不得自建互联网出口。因特殊情况确需单独建设互联网出口的，应当报经领导小组同意，领导小组办公室审批。

所有终端、设备、软件和系统均需设置符合要求的登录密码，删除不需要的用户。在满足运行需要的前提下，采用最小化用户权限分配原则，禁用不必要的服务。

第九条 各处室应当给授权访问人员分配唯一、高强度、定期更新密码的操作账号，实现操作行为可定位、溯源。不得多人共用一个操作账号。

第十条 市大数据局办公网络的 IP 地址按照统一规划进行组织分配和登记信息，并统一进行网络接入设备的配置，各处室不得随意更改。终端设备报废时，按照统一组织销毁的原则，作好备案登记。

第十一条 各处室办公设备接入局办公网络应当进行网络安全检查。各第三方服务团队使用的办公设备由对应责任处室负责管理，如需接入局办公网络的，应当按照规定报领导小组办公室同意后方可接入。

所有接入局办公网络的终端设备均应安装正版软件和正版杀毒防护软件，并及时更新升级防护程序、病毒库和操作系统补丁。

第十二条 各处室加强数据备份工作，对重要数据应定期进行备份，防止因数据备份不及时、不完整等原因造成数据丢失。

第十三条 各处室要严格控制可以访问重要数据的人员数量和帐号。不得将数据资源以任何未授权方式存储到个人存储介质和带离工作环境。

所有使用人不得以任何未授权方式对数据资源进行新增、查询、修改、删除、复制、转移等操作，不得将数据资源在授权工作范围之外以任何方式进行使用。

所有使用人在履行职责中知悉的个人隐私、个人信息、商业秘密、涉密涉敏信息等数据应当依法予以保密，不得泄露或非法向他人提供。严格控制共享数据使用范围，不得擅自转让给第三方使用。

第十四条 在使用和处理数据过程中，因数据汇聚、关联分析等原因，可能产生涉密、涉敏数据的，应当进行安全评估，征求相关专家的意见，并根据评估和征求意见情况采取相应的安全措施。

第十五条 市电子政务外网为非涉密网络，各处室通过网络开展不涉及国家秘密的业务。各处室不得接入涉密计算机、涉密网络设备，不得在市政务外网上传输、处理和存储涉密信息，不得使用涉密存储介质。

所有接入市电子政务外网的业务应用系统要采用数字证书的，应使用国家政务外网数字证书。

各处室不得随意更改市电子政务外网的接入线路和网络接入设备的配置。

第十六条 市大数据局信息按照规范流程进行发布，严格执行信息发布登记、审核制度，原则上在每类信息发布渠道上只有一个信息发布主体账号，降低网络数据安全风险。

各处室在平台发布信息需经统一审核。

第十七条 各处室按照职能加强局管理的信息平台（网站、微信公众号、微博、视频号、小程序、短信平台及应用等）和政

府端、服务端的安全监管，传播社会主义核心价值观，督促相关建设方或运营方及时发现和消除网络安全漏洞和隐患，提高信息平台、终端的安全防护能力。

第十八条 市大数据局加强一体化智能化公共数据平台（宁波城市大脑）的安全管理，建立落实安全制度，严格落实网络安全数据安全保护措施，做好网络攻击的安全防护。

一体化智能化公共数据平台不得部署涉密信息系统和使用涉密信息。

一体化智能化公共数据平台资源不得用于与申请项目无关的用途，或自行转让给第三方使用。不得通过非正常手段或在非授权情况下以桥接、代理等方式来管理和使用一体化智能化公共数据平台的服务和资源。

第十九条 市大数据局管理的机房进出人员应当进行登记审批，并由机房维护人员陪同进出。不得带领未授权人员进入机房任何区域，进行拍照、录像、考察、参观等活动。

货物进出机房应当进行登记审批。设备在机架上的安装位置应当有统一规划，设备安装应当在设备登记的指定位置，不允许安装人员私自改变安装位置。

加强机房相关的门禁卡、密码等物品和信息管理。

第二十条 各处室定期组织对本部门管理的信息系统资产进行全面梳理，明确专人维护管理，做到有台账、有记录，及时

释放过期、僵尸资源，并将清查底数情况及时报领导小组办公室备案。

第二十一条 各处室定期组织对本部门信息管理系统管理及落实情况进行自查，重点检查主机资源、信息系统日常管理机制和安全管理机制是否建立落实。

第二十二条 各处室落实等级保护措施，根据等级保护要求，对信息系统定期组织进行安全状况检测、风险评估和整改加固，重点检查是否存在高危端口、高危漏洞、高危口令、异常账号、异常操作、感染病毒等情况。

加强对网络信息系统等级保护的指导，在组织全市电子政务领域的数字化资源普查中，将电子政务领域信息系统等级保护定级备案情况纳入普查范围。

第二十三条 除不可抗力造成的服务中断外，各系统应按照设计要求不间断运行。如确需临时中断信息系统服务且影响较大时，或长时间关停系统服务，各处室应提前向领导小组报备，并通知受影响的其他单位。

第二十四条 对于机房、政务云等重要系统和设施的日常运维管理实行7*24小时值班和每日零报告制度。重大活动和突发事件期间，相关应急保障按照有关规定执行。

第二十五条 领导小组办公室定期组织技术力量进行网络信息安全技术检测，并督促相应的责任处室进行整改。

第二十六条 加强局网络数据安全力量整合,统筹安排相关安全经费。

第二十七条 处室、个人违反本细则规定,由领导小组办公室责令限期整改,逾期未整改或整改不到位的,报领导小组同意后,进行通报;造成安全隐患或者导致信息安全一般事件发生的,对处室负责人约谈;工作人员违法违规的,依法依规予以处理。

第二十八条 本细则由市大数据局网络信息安全工作领导小组办公室进行解释。

第二十九条 本细则自发布之日起执行。

附件

宁波市大数据发展管理局网络数据安全 安全管理处室责任表

处室名称	主要责任
发展规划处	负责局信息发布平台的信息发布审核工作，负责局信息发布平台网络数据安全的统筹管理、局办公网络和办公设备网络数据安全的统筹管理、其他相关网络数据安全管理工作。
数据资源处	负责公共数据安全管理工作，组织全市电子政务领域的数字化资源普查工作，其他相关网络数据安全管理工作。
应用推进处	负责市政府门户网站的网络数据安全管理工作、浙里办宁波平台的网络数据安全管理工作，其他相关网络数据安全管理工作。
数字基础设施和安全处	承担局网络信息安全工作领导小组办公室工作，负责局网络信息安全日常管理，牵头编制并组织实施局网络安全总体应急预案和年度工作方案、组织开展应急演练，组织或协同网信、公安等部门开展网络信息安全检查，开展服务商网络安全背景审查，组织网络数据安全培训，组织开展网络数据安全重保活动，定期组织技术力量进行网络信息安全技术检测，负责一体化智能化公共数据平台（宁波城市大脑）安全管理工作，其他相关网络数据安全管理工作。
智慧城市建设处	负责基层社会治理平台的网络数据安全、市民卡网络数据安全的统筹管理，其他相关网络数据安全管理工作。
市大数据管理服务中心	负责局管理机房的网络数据安全管理工作、浙政钉宁波平台的网络数据安全管理工作、市电子政务网络的日常网络数据安全管理工作，做好全局网络数据安全的支撑工作，其他相关网络数据安全管理工作。
市智慧城市规划标准发展研究院	负责院办公网络和办公设备的日常网络数据安全管理工作，其他相关网络数据安全管理工作。

抄送：各区县（市）大数据局（中心），开发园区管委会办公室，市级有关单位。

宁波市大数据发展管理局

2021年8月20日印发