

兰州新区管委会办公室文件

新政办发〔2021〕42号

兰州新区管委会办公室 关于印发《兰州新区政务数据资源共享管理办法 (试行)》《兰州新区新型智慧城市基础 平台安全管理办法(试行)》的通知

新区各园区管委会,各部门、各单位,新区各国有集团公司,省属驻区各单位:

《兰州新区政务数据资源共享管理办法(试行)》和《兰州新区新型智慧城市基础平台安全管理办法(试行)》已经兰州新区2021年第32次管委会会议审议通过,现印发给你们,请认真贯彻执行。

兰州新区管委会办公室

2021年9月14日



兰州新区政务数据资源共享管理办法(试行)

第一章 总 则

第一条 为促进兰州新区政务数据资源优化配置和高效利用,充分发挥甘肃政务服务网兰州新区子站等平台作用,推动政府部门之间数据共享和业务协同,切实提高行政效能、服务质量和管理水平,根据《国家数据共享交换平台(政务外网)服务接口申请、授权和使用管理暂行办法》(发改办高技〔2018〕905号)《甘肃省人民政府办公厅关于印发甘肃省政务信息系统整合共享实施方案的通知》(甘政办发〔2017〕167号)和《甘肃省人民政府办公厅印发〈关于建立健全政务数据共享协调机制加快推进数据有序共享的实施方案〉的通知》(甘政办发〔2021〕76号)等有关法规、政策和技术标准,结合兰州新区实际制定本办法。

第二条 本办法所称政务数据资源,是指兰州新区各园区、各部门、各单位、省属驻区各单位、各镇党委和政府、各国有关集团公司(以下统称“各部门”)等,授权、受委托行使行政职能的组织在履行职责过程中产生、采集的非涉密数据。

第三条 本办法所称兰州新区政务大数据共享交换平台(以下简称“政务数据共享平台”),是指兰州新区智慧城市政

务大数据共享交换平台,该平台为各部门之间数据归集、共享、管理等提供技术支撑,包括:政务数据资源运行平台、共享目录体系和交换体系等,通过兰州新区电子政务外网实现国家、省市、新区和园区间互联互通。共享目录体系是各部门之间数据共享的依据,交换体系是各部门之间数据交换的枢纽。

第四条 本办法所称数据共享类别,是指按数据共享程度对政务数据资源的划分方式,分为三类:

(一)可供各部门无条件共享的,为非受限共享类数据;

(二)只能按照特定方式或提供给指定对象共享的,为受限共享类数据;

(三)依照法律、法规、规章规定不能共享的,为非共享类数据。与跨部门并联审批、协同办公、综合管理等相关的政务数据资源,各部门应当提供共享。

第五条 本办法所称数据共享模式,是指在政务数据共享平台归集的政务数据资源提供给各部门共享使用的方式,分为三类:

(一)通过调用验证服务接口进行比对,获取验证结果的比对验证模式;

(二)通过调用查询服务接口,获取或引用查询对象相关数据的查询引用模式;(三)直接下载或通过政务数据共享平台获取批量数据的批量复制模式。

第六条 兰州新区辖区内政务数据资源采集、归集和共

享活动适用本办法。

第二章 政务数据共享原则

第七条 政务数据资源共享应遵循以下原则：

（一）规范采集原则。各部门按照一数之源、多元校核、动态更新的要求和统一的标准规范，采集和处理数据。可以通过共享方式确认或获取的数据，不得另行重复采集，不得擅自超范围采集数据。

（二）无偿提供原则。各部门在履行职责过程中获取、产生的数据资源，是政务数据资源的组成部分。各部门应当无偿为政务数据共享平台及其他部门提供政务数据共享，及时响应其他单位提出的共享需求，配合向政务数据共享平台提供行政权力事项办件、批文、证照、数据报表、决策分析等共享数据。

（三）平台归集原则。共享数据通过政务数据共享平台归集到基础数据库和专业数据库，统一向各部门提供数据共享服务。

（四）按需共享原则。各部门共享使用其他部门的政务数据资源，应当符合部门职能和履职需求，不得超越职能获取和使用其他部门的政务数据资源，不得用于任何其他目的。未经数据提供单位同意，各部门不得擅自向社会发布和公开所获取的共享信息，属于政府信息公开范围内的信息除外。

(五)安全可控原则。各部门应当加强政务数据资源安全管理,不得滥用、非授权使用、未经许可扩散所获取的政务数据资源,因使用不当造成安全问题的,依法追究使用单位及相关责任人的责任。新区党工委办公室、公安局、科技发展局根据职责分工,加强对数据归集、共享过程的安全管理,切实做好数据安全保障工作。法律、法规、规章对政务数据资源共享管理工作另有规定的,从其规定。

第三章 职责分工

第八条 兰州新区数字政府建设统筹推进领导小组负责新区政务数据资源共享工作的组织领导,协调解决和数据共享有关的重大问题。

第九条 新区科技发展局负责政务数据资源共享工作的统筹规划,负责编制《兰州新区政务数据资源共享和开放目录》(以下简称《数据共享目录》);科文旅集团负责政务数据共享平台的建设、升级和运维;负责新区政务数据资源共享管理,定期对政务数据资源工作进行检查评估,配合制定相关标准规范等。

第十条 各部门按照统一规划,负责维护本单位共享目录及内容,负责本单位数据采集、提供和更新工作,并按照有关法律、法规和政策要求,充分利用省级和新区数据共享平台开展政务数据资源共享交换工作和使用所获取的共享数据。

第四章 数据目录

第十一条 新区科技发展局根据各部门的法定职责,参照《兰州市政府数据资源目录编制指南》,组织编制新区《数据共享目录》,包括:数据名称、数据格式、共享类别、共享范围、更新频度、时效要求、提供方式、提供单位、可否向社会开放等内容,经政务信息资源共享工作主管部门审核后在政务数据共享平台上公布实施。

第十二条 各部门要建立健全本单位《数据共享目录》管理制度,明确负责《数据共享目录》的登记、审核、发布、更新等具体工作。

第十三条 各部门在政务数据共享平台上开通、维护本单位的目录系统,按照相关标准及时逐条登记、审核政务数据资源,确保目录内容的完整性、逻辑的一致性、命名的规范性。

第十四条 各部门每年对本单位《数据共享目录》内容进行一次以上维护和整理,可供共享的数据或共享需求发生变化时要及时更新,依规审核后予以发布。

第十五条 各部门应当根据《数据共享目录》,加强政务数据资源管理,规划本单位智慧电子政务应用,开展政务服务协同应用。

第五章 数据采集

第十六条 各部门应当根据《数据共享目录》和本单位工

作要求,在职能范围内采集数据,明确数据采集、发布和维护的规范和程序,建立健全数据更新机制,及时维护相关数据,确保共享数据的真实性、完整性、时效性。

第十七条 各部门使用数据,应当优先从政务数据共享平台共享;需要下级单位采集或提供数据的,要与下级对口部门衔接,不得要求下级对口部门重复采集各部门已共享的数据。

第十八条 各部门在数据采集过程中,应当主动通过政务数据共享平台与其他单位的相关数据进行比对,发现数据不一致时,要及时修改;部门间有分歧的,由政务信息资源共享工作主管部门协调核实。

第十九条 各部门应当以数字化方式采集、记录和存储数据,同时将具备条件的数据进行结构化处理,并通过数据库进行管理。非数字化数据应按照相关技术标准开展数字化改造。

第二十条 各部门应当对文书类、证照类数据加盖新区统一的电子印章,以保证数据不可更改。

第二十一条 各部门采集、办理并提供共享的网上审批类、文书类及证照类电子材料,应当依据有关规定及时归档。具有永久保存价值的电子材料,归档时应同时保存电子和纸质版本。

第六章 数据归集

第二十二条 新区科技发展局协同新区各相关部门和科技文化旅游集团有限公司,利用省市政府统建的人口、法人单位、自然资源和空间地理、宏观经济、电子证照库、权力事项库、办件库等基础数据库,通过省交换平台将数据同步到新区政务数据共享平台,形成新区基础数据库。专业数据库由业务部门负责在政务数据共享平台上建设和维护,统一为各部门提供政务数据资源共享服务。

第二十三条 各部门应当将共享数据所对应的原始数据库集中部署在政务数据共享平台,通过统一的数据访问接口向其他各部门提供服务。同时,政务数据共享平台内的共享数据统一交换到省、市共享平台上,为各级各部门履行公共管理和服务职能提供支持。

暂时无法集中部署的数据库,必须按统一标准,向政务数据共享平台提供数据访问接口。

第二十四条 各部门向政务数据共享平台归集的共享数据,应按照《兰州市政府数据隐私保护和安全审查工作指南》等规定,事先经过本单位的保密审查,不得涉及国家秘密。其中:自然人数据应当以法定身份证件作为标识提供;法人及其他机构数据应当以组织机构代码作为标识提供;没有组织机构代码的市场经营主体应当以营业执照作为标识提供。

第二十五条 各部门对所提供的政务数据资源进行实时动态管理,其中:电子证照、文书类数据应当进行实时更新;其他业务数据应当在产生后2个工作日内进行更新;情况特殊的,各部门应当经政务信息资源共享工作主管部门审核后,每季度首月上旬进行更新。

第七章 数据共享应用

第二十六条 各部门应主动通过政务数据共享平台获取履行职能所需要的数据,以联机方式实现与其他部门的数据共享与业务协同,实现精细化服务和管理,提升公共服务、社会治理和联合监管能力。

第二十七条 各部门应当通过政务数据共享平台的前置交换系统发布共享数据,并在目录系统中注册受限或非受限共享数据目录。

第二十八条 各部门通过政务数据共享平台的目录系统检索、发现、定位和申请履行职能所需要的数据,受理其他部门使用本单位受限共享数据的申请。

第二十九条 各部门使用非受限共享类数据时,通过政务数据共享平台选取,即时完成共享。

第三十条 各部门使用受限共享类数据,需通过政务数据共享平台向数据提供单位提出申请。数据提供单位以履行职责需要为主要依据,审核共享需求,确定使用对象、所需数

据项、数据共享模式等要素,确保按需安全共享。

数据需求方提出申请后,对于无条件共享的数据,由新区共享交换平台管理单位进行审核,审核通过后在2个工作日内直接将共享数据交换到数据需求方;对于有条件共享的数据,由新区共享交换平台管理单位进行初审后,流转数据提供方进行办理,数据提供方应在3个工作日内完成审批(审批不通过的应说明具体理由),授权新区共享交换平台管理单位提供共享数据,新区共享交换平台在得到授权后的2个工作日内将共享数据交换到数据需求方。

对共享条件、申请理由、授权结果等存在意见分歧的,由政务信息资源共享工作主管部门召集数据提供方、数据需求方和共享交换平台建设管理单位协商解决,无法协商一致的,报请领导小组协调解决。

数据需求方对获取的共享数据有疑义或发现有明显错误的,应在发现问题1个工作日内反馈至数据提供方予以校核,数据提供方应在3个工作日内予以处理和回复。

第三十一条 各部门应当利用共享的基础数据库或专业数据库,清洗、比对本部门业务数据库。对不一致或错误的数据库,进行核查或纠错,并在3个工作日内向对方反馈数据。

第三十二条 各部门通过政务数据共享平台获得的加盖电子印章文书类、证照类政务数据,与纸质文书具有同等效力。法律、法规另有规定的,从其规定。

各部门可以将通过共享方式获得的文书类、证照类等政务数据作为办事和执法依据。法律、法规规定不适用电子文书的除外。

各部门可以通过电子方式确认的事项和获取的材料,不得要求行政管理相对人确认并提交。法律、法规另有规定的,从其规定。

第八章 安全管理

第三十三条 按照“谁提供、谁负责,谁流转、谁负责,谁使用、谁负责”的原则,加强数据共享全过程安全管理。

(一)数据提供方应按照国家信息安全等级保护要求,对政务信息系统进行安全管理和防护,保障本部门数据和服务接口安全。

(二)共享交换平台建设管理单位应按照国家信息安全等级保护要求,对共享交换平台进行安全管理防护,加强安全传输、访问控制、授权管理和全流程审计,保障政务信息资源共享交换时的数据安全。

(三)数据需求方应按照国家信息安全等级保护要求,加强服务接口调用的用户权限管理、访问控制和日志审计,确保接口访问安全和数据授权使用。

第三十四条 各部门应当建立健全本单位政务数据资源业务管理、安全管理及责任追究等规章制度,并指定分管领

导、牵头科室和专人负责政务数据资源共享、保密审查和风险防范等工作,切实完善安全技术保障体系,确保共享数据安全。出现安全问题时,应及时向信息安全行政主管部门报告,并配合相关职能部门处置。

第三十五条 政务数据共享平台应当严格执行信息网络安全和保密等有关法律、法规和政策规定,并按国家技术规范和标准,定期对政务数据共享平台进行信息安全风险评估,排查安全风险和隐患,建立身份认证、存取访问控制、审计跟踪等机制,确保共享数据可用、完整、安全、保密。

第三十六条 新区科技发展局协同科技文化旅游集团有限公司制定完善政务数据共享平台运行管理维护制度、灾备恢复机制和应急处置预案,定期开展应急演练,确保平台安全、稳定、可靠运行。

第九章 监督考核

第三十七条 政务数据资源共享工作纳入新区“数字政府”建设目标管理。新区科技发展局负责政务数据共享平台的日常监管,定期对各部门提供的数据数量、质量及更新、使用等情况进行综合评估,并公布评估结果、提出改进意见。

第三十八条 新区财政局(国资监管局)将政务数据资源共享情况作为安排政务信息化系统建设资金的重要依据;对不响应数据共享的部门,以新区科技发展局提供的名单,暂停

安排其相关新建项目和运维费用。

第十章 附 则

第三十九条 本办法由兰州新区科技发展局负责解释。

第四十条 本办法自印发之日起施行,有效期 2 年。

兰州新区新型智慧城市基础平台安全管理办法

(试 行)

第一章 总 则

第一条 为进一步规范新区新型智慧城市基础平台使用管理、提升政务服务安全水平,根据国家、省、市相关法律法规和文件精神,结合新区实际,制定《兰州新区新型智慧城市基础平台安全管理办法(试行)》,对新区 eLTE 市政无线专网、电子政务外网、电子政务协同办公系统、政务大数据共享交换平台和政务服务联动审批系统、电子印章、电子证照等新型智慧城市信息化平台和系统运维进行科学化、规范化管理。

第二条 根据《中华人民共和国网络安全法》《中华人民共和国无线电管理条例》《中华人民共和国政府信息公开条例》《中华人民共和国电子签名法》《中华人民共和国计算机信息系统安全保护条例》《中华人民共和国突发事件应对法》《国家信息化领导小组关于加强网络与数据安全保障工作的意见》《工业和信息化部关于 1447—1467 兆赫兹(MHz)频段宽带数字集群专网系统频率使用事宜的通知》《国家政务服务平台网络安全保障要求》《国务院办公厅关于建立健全政务数据共享协调机制加快推进数据有序共享的意见》《国务院关于地

方各级人民政府和部门印章管理的规定》《国家政务服务平台电子证照跨区域共享服务接入要求》《甘肃省深入推进“互联网+政务服务”工作方案》《甘肃省一体化在线政务服务平台电子印章管理实施办法(试行)》《甘肃省一体化在线政务服务平台电子证照管理实施办法(试行)》《甘肃省人民政府办公厅印发〈关于建立健全政务数据共享协调机制加快推进数据有序共享的实施方案〉的通知》及相关法律法规和技术标准,结合新区实际,制定本办法。

第二章 eLTE 市政无线专网管理

第一节 分 则

第三条 兰州新区基于 4G 网络 TD-LTE 的 eLTE 市政无线专网,支持语音、数据、图像和视频等多种业务的不同传输速率,兼容窄带集群系统的同时,向宽带化平滑过渡,构建各种通信系统相融合的新一代宽带无线多媒体集群通信系统,服务城市治理、公共事业、智慧产业发展,满足新区公安、应急、教育、医疗、能源等智慧应用对无线回传业务的需求。

第四条 eLTE 市政无线专网管理、运行和维护按照“谁建设、谁管理、谁运维”的原则,实行分级管理、分层负责。

第二节 职责分工

第五条 取得无线电频率使用许可,应当符合下列条件:

(一)所申请的无线电频率符合无线电频率划分和使用规

定,有明确具体的用途;

(二)使用无线电频率的技术方案可行;

(三)有相应的专业技术人员;

(四)对依法使用的其他无线电频率不会产生有害干扰;

(五)法律、行政法规规定的其他条件。

第六条 新区科技发展局是新区 eLTE 市政无线专网的主管部门,负责规划实施、监督管理、业务指导等工作;新区科技文化旅游集团有限公司负责 eLTE 市政无线专网的建设运维、安全保障、综合协调和业务培训工作,负责核心平台骨干网络、核心机房及各接入单位 eLTE 市政无线专网边界设备的运行维护。新区科技发展局和科技文化旅游集团有限公司共同承担职责:

(一)负责贯彻落实国家、省、市和新区无线电管理相关法律法规规定,接受国家、省、市、新区无线电管理委员会等管理机构的指导、监管,完成纵向业务系统的联通;

(二)负责新区 eLTE 市政无线专网总体规划和相关制度、标准的制定及贯彻落实;

(三)负责核准新区 eLTE 市政无线专网接入及接入单位相关服务调整、交更、报备,并为网络故障、网络设施等提供第一时间技术支持;

(四)负责对新区 eLTE 市政无线专网进行网络安全统一规划和管控,确保网络及信息安全;

(五)组织开展业务培训。

第七条 eLTE 市政无线专网接入单位职责：

(一)按照国家有关法律、法规和本办法，制定本单位 eLTE 市政无线专网分级管理、网络安全、应急处置等配套规章制度。

(二)建立本单位 eLTE 市政无线专网管理组织体系，确定分管领导和专(兼)职管理人员，明确工作职责分工，建立专网及设备管理使用台帐，并报新区科技发展局备案。

(三)负责本单位 eLTE 市政无线专网及设备使用申请及报备，做好专网相关设备设施的日常管理和运行维护，定期将网络及业务系统运行情况报送新区科技发展局。

(四)负责本单位网络安全管理，做好涉及重要业务系统的数据备份工作，及时报送协调处理突发性网络故障信息，确保网络稳定运行。

(五)安装核心网的接入单位，负责做好机房出入、机房供电、机房环境卫生、设备点检和巡检等日常管理，保证机房设备运行环境安全、稳定。

第八条 任何其它单位或个人不得擅自挪用、挤占、拆除 eLTE 市政无线专网设备；不得随意更改 eLTE 市政无线专网接入设备配置；不得擅自切断 eLTE 市政无线专网设备电源、挪动相关设备、切断或移动相关通信传输线路。

第三节 无线电频率管理

第九条 使用无线电频率应当遵守国家、省、市和新区无线电管理的有关规定和无线电频率使用许可证的要求,接受、配合无线电管理机构的监督管理。

第十条 无线电频率使用许可证应当妥善保存,任何组织或者个人不得伪造、涂改、冒用无线电频率使用许可证。

第十一条 国家根据维护国家安全、保障国家重大任务、处置重大突发事件等需要依法实施无线电管制的,管制区域内的无线电频率使用人应当遵守有关管制规定。

第十二条 无线电频率使用人不得擅自转让无线电频率使用权,不得擅自扩大使用范围或者改变用途。

第十三条 依法使用的无线电频率受到有害干扰的,可以向无线电管理机构投诉,无线电管理机构应当及时协调处理,并将处理情况告知投诉人。

第十四条 无线电频率使用人拟变更无线电频率使用许可证所载事项的,应当向作出许可决定的无线电管理机构提出申请。符合法定条件的,无线电管理机构应当依法办理变更手续。

第四节 网络安全管理

第十五条 eLTE 市政无线专网上软件及信息资源的使用应遵守有关知识产权管理的法律法规。eLTE 市政无线专网上的信息资源(主要指数据库资源、软件和内部信息等)属

于各信息发布单位所有,任何单位和个人使用相关信息资源必须通过信息发布单位的许可后方可使用。法律法规有其他规定的除外。

第十六条 新区科技发展局牵头、新区科技文化旅游集团有限公司具体负责做好 eLTE 市政无线专网网络管理员的网络安全等培训。

第十七条 接入 eLTE 市政无线专网的设备状况和网络设置每月至少检查 1 次,并建立运行日志(日志保存期不得少于 6 个月),按规做好日常点巡检,对重要文件、数据、操作系统及应用系统应该定期备份。

第十八条 各 eLTE 市政无线专网接入单位必须接受并配合网络安全及保密部门的监督检查。任何单位和个人未经批准,不得从事下列活动:

- (一)对接入 eLTE 市政无线专网设备的参数配置进行修改;
- (二)从事与工作无关的活动而大量占用 eLTE 市政无线专网资源,造成网络拥堵;
- (三)其它任何危害 eLTE 市政无线专网和信息系统安全的活动。

第十九条 各 eLTE 市政无线专网接入单位应积极做好相关网络安全保障工作,包括但不限于安装正版防毒软件并及时更新操作系统补丁等。eLTE 市政无线专网遭受病毒、黑客、木马等非法手段攻击时,各接入单位必须积极配合,会

同科技、网信、公安等部门共同处置网络安全事件。

第二十条 各 eLTE 市政无线专网接入单位必须遵守国家的有关法律、法规,严格执行《中华人民共和国保守国家秘密法》和《计算机信息系统国际联网保密管理规定》等法律法规,不得在 eLTE 市政无线专网上处理和存储任何涉密信息,禁止交叉使用移动存储介质。

第二十一条 各 eLTE 市政无线专网接入单位对上网行为及发布的信息负责,严禁通过 eLTE 市政无线专网发布传播含有下列内容的信息:

- (一)反对宪法所确定的基本原则的;
- (二)危害国家安全,泄露国家秘密,颠覆国家政权,破坏国家统一的;
- (三)损坏国家荣誉和利益的;
- (四)煽动民族仇恨、民族歧视,破坏民族团结的;
- (五)破坏国家民族宗教政策,宣扬邪教和封建迷信的;
- (六)散布谣言,扰乱社会秩序,破坏社会稳定的;
- (七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的;
- (八)侮辱或者诽谤他人,侵害他人合法权益的;
- (九)含有法律、行政法规禁止的其他内容的。

各 eLTE 市政无线专网接入单位如发现 eLTE 市政无线专网上存在有害信息时应保留原始记录,并及时向新区网信

等相关部门报告。

第二十二条 建立 eLTE 市政无线专网安全事件报告制度。eLTE 市政无线专网接入单位发现网络安全事件,应初步查明原因后及时向新区科技发展局报告。

第二十三条 eLTE 市政无线专网运营单位每年至少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检测评估一次,并将检测评估情况和改进措施报送负责关键信息基础设施安全保护工作的相关部门。

第三章 电子政务外网管理

第一节 分 则

第二十四条 为规范对兰州新区电子政务外网(以下简称“政务外网”)的管理,保证政务外网安全、可靠、高效运行,根据《中华人民共和国网络安全法》《国家信息化领导小组关于推进国家电子政务网络建设的意见》《国务院办公厅关于促进电子政务协调发展的指导意见》《国家电子政务外网信息安全标准体系框架》及国家、省、市电子政务外网有关规定,结合新区实际,制定本办法。

第二十五条 政务外网是电子政务建设的基础,是利用先进计算机和网络通信技术,实现各部门之间及部门内部计算机联网、信息资源共享,促进政府职能管理现代化、信息化的计算机信息基础网络。政务外网为非涉密网络,严禁传输、

处理涉密信息。政务外网与互联网逻辑隔离,通过安全设备与互联网联接。政务外网主要承载各级政务部门社会管理、公共服务和部分办公业务。

第二十六条 政务外网按照“统一网络平台,统一互联网出口”的原则进行建设和管理,由核心网络平台和各接入点组成,其中核心网络平台上联省级政务外网,下联各党政机关单位及直属事业单位政务外网。各党政机关单位、直属事业单位和村(社区)原则上必须接入政务外网,不再独立铺设和组建传输骨干网,不再单独设置互联网出口。各单位专网运行的信息系统,应按照国家、省、市相关要求,逐步向政务外网迁移。

第二十七条 政务外网的管理、运行和维护按照“谁建设、谁管理、谁运维”的原则,实行分级管理、分层负责。

第二节 职责分工

第二十八条 新区科技发展局是新区政务外网的主管部门,负责政务外网的规划实施、监督管理、业务指导等工作。新区科技文化旅游集团有限公司负责新区核心平台骨干网络 and 核心机房的建设运维、安全保障、综合协调、业务培训及各接入单位政务外网边界设备的运行维护。各园区负责辖区内乡镇(中心社区)、村(社区)网络链路的建设运维和安全管理等工作。新区科技发展局和科技文化旅游集团有限公司共同承担以下职责:

(一)接受国家、省电子政务外网管理机构指导、监管,完

成纵向业务系统的联通；

(二)负责新区政务外网有关制度、标准的制定和贯彻落实,制定新区政务外网总体规划；

(三)负责新区政务外网建设、管理和运行维护,核准新区政务外网接入和对接入单位的相关服务调整、交更、报备,并为网络故障、网络设施等第一时间提供技术支持；

(四)负责新区政务外网网络地址统一规划、管理、分配和网络安全管控；

(五)组织开展业务培训。

第二十九条 政务外网接入单位职责：

(一)按照国家有关法律、法规和本办法,制定本单位政务外网分级管理、网络安全、应急处置等配套规章制度。

(二)按照新区统一规划和标准,建立本单位政务外网管理组织体系,确定分管领导和专(兼)职管理人员,明确工作职责分工,并报新区科技发展局备案。

(三)负责本单位政务外网和设备使用申请及报备,做好外网相关设备设施的日常管理和运行维护,定期将网络及业务系统运行情况上报新区科技发展局。

(四)负责本单位网络安全管理,做好重要业务系统的数据备份工作,及时上报协调处理突发性网络故障信息,确保网络稳定运行。

(五)安装核心网的接入单位,负责做好机房出入、机房供

电、机房环境卫生、设备点检巡检等日常管理,保证机房设备运行环境安全、稳定。

第三节 接入管理

第三十条 政务外网接入单位(以下简称“接入单位”)实行规范化管理,未经允许的任何单位和个人不得接入政务外网。申请接入单位提交入网申请和接入方案,新区科技发展局负责对接入单位的资格和接入方案进行审核,审核通过后指导完成接入。

第三十一条 政务外网用户的 IP 地址由新区科技发展局进行统一规划、管理。未经授权,用户的 IP 地址不得更改。

第三十二条 新区科技发展局牵头、新区科技文化旅游集团有限公司负责建立接入网络、接入系统的档案,包括接入单位责任人、接入网络和系统的基本情况、统一分配的通信端口、网络地址及域名等。

第三十三条 为确保政务外网安全,政务外网的互联网出口实行统一管理,有独立互联网出口的单位或部门不得直接接入政务外网。确需接入的单位应向新区科技发展局提交书面申请和按规办理接入手续,并做好边界防护。

第三十四条 任何其它单位或个人不得擅自挪用、挤占、拆除政务外网设备;不得随意更改政务外网接入设备配置;不得擅自切断政务外网设备电源、挪动相关设备和切断、移动相关通信传输线路;不得擅自和其他网络对接;不得以互利为目

的占用政务外网资源。

第三十五条 各接入单位应做好网络故障先期处置工作。发现政务外网状况异常时,首先由本单位网络管理员进行自查并处置,如无法排除故障,应及时上报新区科技发展局进行协调处理。

第三十六条 各接入单位应积极有效地利用政务外网开展工作,提高管理的自动化水平,发挥政务外网高速、移动、安全的作用,各级部门在开展电子政务应用系统建设时,要充分利用政务外网平台。

第四节 网络安全管理

第三十七条 各接入单位在政务外网上新增或变更业务系统、变动 IP 地址、设置虚拟专网或占用其它网络资源的,必须向新区科技发展局提出书面申请,经核准后方可实施。

第三十八条 政务外网上软件及信息资源的使用应遵守有关知识产权管理的法律法规。政务外网上的信息资源(主要指数据库资源、软件和内部信息等)属于各信息发布单位所有,任何单位和个人使用相关信息资源必须通过信息发布单位许可后方可使用。法律法规有其他规定的除外。

第三十九条 新区科技发展局牵头、新区科技文化旅游集团有限公司具体负责,做好政务外网接入单位网络管理员的网络安全培训。

第四十条 各接入单位每月至少对接入政务外网的设备

状况和网络设置检查 1 次,并建立运行日志(日志保存期不得少于 6 个月),对重要文件、数据、操作系统及应用系统至少每月进行一次备份。

第四十一条 各接入单位必须接受并配合网络安全及保密部门的监督检查。任何单位和个人未经批准,不得从事下列活动:

(一)对接入政务外网设备的参数配置进行修改。

(二)从事与工作无关的活动而大量占用政务外网资源,造成网络拥堵。

(三)其它任何危害政务外网和信息系统安全的活动。

第四十二条 各接入单位应积极做好相关网络安全保障工作,包括但不限于安装正版防毒软件并及时更新操作系统补丁等。政务外网遭受病毒、黑客、木马等非法手段攻击时,各接入单位必须积极配合,会同网信、公安等部门共同处置网络安全事件。

第四十三条 各接入单位必须遵守国家有关法律法规,严格按《中华人民共和国保守国家秘密法》和《计算机信息系统国际联网保密管理规定》等规定,做到政务外网物理隔离,不得在政务外网上处理和存储任何涉密信息,禁止交叉使用移动存储介质。

第四十四条 各接入单位对上网行为及发布的信息负责,严禁通过政务外网发布传播含有下列内容的信息:

- (一)反对宪法所确定的基本原则的；
- (二)危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；
- (三)损坏国家荣誉和利益的；
- (四)煽动民族仇恨、民族歧视，破坏民族团结的；
- (五)破坏国家民族宗教政策，宣扬邪教和封建迷信的；
- (六)散布谣言，扰乱社会秩序，破坏社会稳定的；
- (七)散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；
- (八)侮辱或者诽谤他人，侵害他人合法权益的；
- (九)含有法律、行政法规禁止的其他内容的。

各政务外网接入单位如发现政务外网上存在有害信息时应保留原始记录并及时向新区科技发展局报告。

第四十五条 建立政务外网安全事件报告制度，接入单位发现网络安全事件，应初步查明原因后半小时内向新区科技发展局报告。

第四十六条 接入政务外网的信息化系统安全标准应不低于政务外网标准。安全标准偏低、安全边界不清、溯源能力不足、日志记录不全的系统或设备不得接入政务外网。

第四十七条 政务外网的运营者每年至少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检测评估一次，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。

第四章 电子政务协同办公系统管理

第一节 分 则

第四十八条 协同办公系统是管委会统一规划建设,为新区各有关单位线上公文收发和工作人员工作、学习、交流提供服务的办公信息平台。

第二节 系统运行管理

第四十九条 新区管委会办公室负责协同办公系统应用的组织、协调、指导和督促落实工作。新区管委会各部门及各集团公司负责对本单位文件进行管理,应积极利用电子政务外网和协同办公系统开展工作,并提出进一步完善系统的意见和建议。

第五十条 新区科技发展局牵头、新区科技文化旅游集团有限公司具体负责协同办公系统的建设、运行维护和日常管理。

第五十一条 各接入单位使用协同办公系统,必须在新区电子政务外网网络环境运行,确保网络信息安全。

第五十二条 各接入单位使用协同办公系统用户权限由新区管委会办公室根据工作实际统一分配,经审核符合要求的电脑和用户方可入网运行。因工作需要,确需增加用户数和用户权限,应向新区管委会办公室提出书面申请,核准后对

入网电脑和用户逐个登记、统一分配。

第五十三条 协同办公系统实行实名制管理,不得在系统上发布与工作无关的公告或信息。

第五十四条 协同办公系统各使用单位网络安全和保密管理要符合国家、省、市相关规定,要健全完善管理制度,明确专人负责,加强网络、密码和接入电脑等终端的管理。

第五十五条 使用协同办公系统电脑需设置密码(密码由字母、数字和特殊符号组成),长时间离开电脑要保存正在处理的文件并锁定电脑,重要文件须定期整理备份。

第三节 线上办公业务管理

第五十六条 协同办公系统主要包括如下主要功能:

公文收发包括省、市等上级来文,应用单位向党工委、管委会报送各类请示性公文,以党工委办公室、管委会办公室名义下发各类文件,新区各部门之间流转公文等。

其他业务包括由党工委办公室、管委会办公室等部门发出各类会议通知及督办催办、会议管理、请假管理、车辆管理等多种业务功能。

第五十七条 在新区管委会范围内,电子文件与相同内容的纸质文件具有同等效力,各部门可将电子文件作为对内对外贯彻执行工作、办理事项的依据。

第五十八条 各应用单位应按要求配备接入协同办公系统的电脑、扫描仪、打印机等终端设备,以满足正常收发文件

资料需要。

第五十九条 各应用单位应当至少明确一名综合素质较高的操作人员,确保及时通过协同办公系统收发文件资料。

第六十条 对涉及秘密及机密级以上的公文,按照国家、省、市相关规定以纸质文件传递,严禁在协同办公系统流转。对非涉密公文,必须通过协同办公系统按程序流转。内部资料、依申请公开及不予公开的文件可以正常流转运行。

第六十一条 各应用单位上班时应全程登陆协同办公系统并保持在线状态,时时检查需办理的事项、公告通知等,确保信息通畅和文件流转及时。如发生系统和网络等故障情况,务必于第一时间报新区科技发展局协调解决,同时向新区管委会办公室报备,积极采取其他方式传输公文,确保工作不受影响。

第六十二条 应用单位要及时下载最新公文,将文件保存至系统盘外的其他硬盘分区内,并根据工作需要决定是否打印。对于紧急重要的公文,收件人员要即收即办,不得延误。

第六十三条 相关人员外出或者出差培训时,可使用手机登录电子政务协同办公系统处理重要流程。外出时间较长者须委托部门其他人员进行业务办理,不得出现人员外出造成主办流程无法流转的情况。

第六十四条 管委会办公室对各应用单位日常公文(含

会议通知)接收和办理等情况进行统计监督,对收报和办理不及时的情况予以通报批评或绩效考核。对由于单位和个人原因造成协同办公系统无法运行或贻误工作的,将追究相关责任人的责任。

第四节 安全保密管理

第六十五条 协同办公系统涉及使用电子印章和人员签名,由新区科技发展局牵头统一制作并授权使用,电子印章的使用、管理与实物印章相同。

第六十六条 有权使用电子印章和人员签名的人员,应定期更换密码,妥善保管,不得泄露;电子印章及签名仅在协同办公系统上与鲜章具有同等效力,纸质打印无效。

第六十七条 严禁下列行为,对违反规定造成不良后果的,将依法依规追究相关责任人的责任:

- (一)严禁未经允许擅自改变电子政务外网线路;
- (二)严禁将协同办公系统用户名、口令转交他人使用;
- (三)严禁无关人员登录协同办公系统收发文件资料;
- (四)严禁盗用他人口令、入侵和破坏协同办公系统;
- (五)严禁利用电子政务外网办公系统发送涉密信息;
- (六)严禁私自将个人电脑或外部人员电脑接入新区电子政务外网。

第五节 系统维护管理

第六十八条 各单位应按照国家网络安全相关法律和行

业标准规范,落实防火墙及网络防病毒软件安装等安全防护措施,避免计算机感染病毒或被网络攻击造成网络安全事故。

第六十九条 各单位管理员应按照规定指导检查本单位计算机安装防病毒软件,并及时更新操作系统安全补丁及病毒特征码。

第七十条 各单位文书应定期整理归档部门文档资料,及时督查文件流转办结情况,删除过期无效文档。使用人员应及时删除在协同办公系统上生成的失效或错发信息。

第五章 政务大数据共享交换平台管理

第一节 分 则

第七十一条 共享交换平台依托兰州新区统一电子政务外网建设,是兰州新区非涉密政务信息资源共享交换的服务载体,可实现新区各部门间政务信息资源在线共享交换,为各级政务部门提供目录查询、资源订阅、数据下载等服务。共享交换平台主要包括:兰州新区政务大数据信息资源综合门户、资源交换平台、统一运行监控平台、资源交换对账系统、智能化运维平台、用户中心、数据治理平台、宏观经济库、决策分析平台等。

第七十二条 本办法适用于共享交换平台政务信息资源目录编制、资源共享、资源申请、资源授权、资源交换等活动。

第七十三条 共享交换平台的用户包括政务信息资源提

供单位、使用单位、管理单位和共享交换平台运维单位的相关人员。

(一)政务信息资源提供单位(以下简称“提供单位”)是指提供查询、核验等数据共享服务的各级政务部门。提供单位负责本部门政务信息资源的采集、资源编目、目录更新、目录维护、数据挂接、数据更新,以及服务接口的开发、注册、发布等工作;对本部门有条件共享数据及需要管控参数的无条件共享服务接口进行使用授权,要明确牵头工作部门、分管负责人,不断完善内部管理机制,优化服务接口授权工作流程,提高数据供给质量和效率。

(二)政务信息资源使用单位(以下简称“使用单位”)是指因履行职责需通过共享交换平台申请使用共享数据的各级政务部门(包括承担行政职能的下属事业单位)。使用单位按照本办法规定,提出共享数据申请,获取共享数据。

(三)共享交换平台管理单位(以下简称“管理单位”)为新区科技发展局,负责建立新区统一的政务信息资源目录体系,实现政务信息资源目录的动态更新、共享校核、权威发布;负责汇总、审核各部门数据共享需求,统一向省级共享交换平台管理部门提出使用申请;组织各部门编制政务信息资源目录,协调、指导和监督新区政务信息资源共享工作。

(四)共享交换平台运维单位(以下简称“运维单位”)为新区科技文化旅游集团有限公司,负责新区数据共享交换平台

的建设管理、培训指导、运营维护和安全保障。运维单位应明确数据共享交换平台技术支持人员及联系方式,根据数据提供单位和使用单位要求,通过平台提供数据共享技术支持和服务保障。

第七十四条 共享交换平台支持结构化数据、非结构化数据、服务接口三种类型的数据资源编目和交换,提供资源获取、资源订阅、资源比对三种资源交换方式与服务。

第七十五条 共享交换平台政务信息资源接入模式分为:文件及文件夹接入、库表接入、服务接口接入。

(一)文件。提供单位将共享数据整理成结构化文档形式,同步至部门侧数据共享前置机,通过共享交换平台提供给数据需求方。文件支持 wps、doc、xml、txt、docx、html、ppt、et、xls、csv 等格式。

(二)库表。提供单位将共享数据同步至部门侧数据共享前置库,由共享交换平台根据数据提供方的授权,以数据库或数据表的方式交换给数据需求方。数据提供方需要及时更新数据内容,并确保共享数据和业务数据的一致性。

(三)服务接口。提供单位负责服务接口的开发,通过部门侧前置机统一对外发布接口,经由共享交换平台代理后,由使用单位通过服务接口地址及参数使用数据。

第二节 管理权限

第七十六条 共享交换平台管理单位负责提供单位、使

用单位在平台使用过程中的协调、监督、管理工作。运维单位负责按照相关规定程序分配系统权限、提供技术支持、做好系统维护等。

第七十七条 使用单位在申请资源或提出资源需求时，应明确信息资源使用用途，提供单位须及时响应并办理资源申请或资源需求申请。使用单位在申请共享交换平台已发布的政务信息资源时，经提供单位审批同意后方可使用，资源使用范围仅限于使用单位申请资源时注明的用途；如因业务需要，需申请共享交换平台未发布的政务信息资源，须向共享交换平台管理单位提出书面申请，经批准后，由运维单位负责指导提供单位将政务信息资源接入共享交换平台发布，并为提供单位分配该资源的审核权限。

第七十八条 申请接入共享交换平台的相关单位需经共享交换平台管理单位核准，由运维单位设置接入权限，指导申请单位完成政务信息资源目录编制、数据接入等工作。

第七十九条 系统管理员由运维单位指定专人担任，其职责主要是根据共享交换平台管理单位要求为用户分配具体权限，负责共享交换平台的日常监控、运维、管理等工作。

第八十条 共享交换平台系统管理员统一设置并分配各单位登录账号，各单位通过用户名及密码的方式登录共享交换平台，首次登录需先修改密码（密码由字母、数字和特殊符号组成），修改完成后方可登录进入平台。

第八十一条 原则上共享交换平台为新区各单位分别分配一个单位管理员账号,由各单位指定专人(各单位共享交换平台管理员)负责,各单位共享交换平台管理员根据本单位内设机构为各业务科室分配一个业务人员使用账号。各单位数据共享工作分管领导、管理员及业务人员情况报管理单位备案。各单位共享交换平台管理员具有本单位范围内的资源编目、需求申请、服务申请、服务授权等操作权限;业务人员使用账号具有资源编目、数据查询、交换申请等权限。

第三节 接入管理

第八十二条 新区各单位依托兰州新区电子政务外网,通过共享交换平台前置机接入共享交换平台,各单位前置机由共享交换平台管理单位统筹配备。

第八十三条 新区各单位共享交换平台的接口需由本单位共享平台管理员负责,并对用户权限进行严格管理,切实做好数据安全防范工作。

第八十四条 运维单位工作中使用到的数据、用户名密码及系统配置信息,不得在与互联网连接的计算机中存储、处理及传输。

第八十五条 运维单位需加强网络监控,若发现计算机或网络遭到大规模的攻击,需立即向共享交换平台管理单位汇报,并及时进行网络隔离,确保平台及数据安全;如发现资料泄露情况,在采取应急措施的同时,应及时将情况上报至共

享交换平台管理单位和新区保密工作管理部门。

第八十六条 运维单位必须遵守信息储存、清除、备份等相关制度,定期开展信息安全检查,并及时更新系统漏洞。针对重要资料需通过技术等手段做好备份工作,以防发生数据资料遗失、损毁等情况。

第八十七条 运维单位需定期进行信息安全和保密管理的监督、检查工作,提高泄密隐患发现能力和泄密事件处置能力,做好信息安全和保密工作。

第八十八条 运维单位系统管理员及运维人员上岗前,用人单位需明确相应的岗位描述、任用条款及其应履行的信息安全职责,并确保其充分理解信息安全职责,保证其所承担的角色符合共享交换平台的信息安全要求。

第八十九条 共享交换平台使用人员调动、离职等工作变动时,须在各单位共享交换平台管理员的监督下完成工作及相关资料交接,包括个人办公电脑中的业务资料交接。工作交接完成后,本单位共享交换平台管理员应及时取消离职人员的系统访问权限,并修改密码。

第九十条 各单位共享交换平台管理员调动、离职等工作变动时,各单位须及时指定新的平台管理员,并做好工作交接和培训,同时上报共享交换平台管理单位备案。

第四节 维护管理

第九十一条 新区各部门必须配合管理单位做好资源编

目、数据上传、数据交换等工作,积极争取国家、省、市对口部门专网及独立系统与共享交换平台互通共享,数据上传共享情况纳入新区绩效考核指标任务。

第九十二条 运维单位应定期检查平台的运行状态、资源交换状态、资源更新状况、设备状态等,并及时处理平台上报的告警事件。

第九十三条 运维单位应定期开展信息安全检查、系统备份工作,并及时更新系统漏洞,检查备份数据的有效性。

第九十四条 运维单位应及时处理各单位反馈的在资源编目、资源审核、数据共享等过程中产生的问题。

第九十五条 运维单位负责维护平台所有设备、数据库以及业务系统,确保平台与系统安全稳定运行,同时应加强对提供单位的技术支持,及时协助提供单位解决系统运行过程中发生的各类技术问题。

第五节 故障处理与应急处置

第九十六条 共享交换平台发生故障时,应当遵循“故障报告、故障处理、故障恢复”的程序进行处置。

第九十七条 共享交换平台核心应用服务器(如交换平台服务器、门户服务器)发生故障或各单位前置服务器发生故障时,运维单位应及时向共享交换平台管理单位通报故障情况,并展开故障排除,原则上故障恢复时限不超过3个工作日,实际工作中可根据具体情况进行调整。

第九十八条 共享交换平台运行过程中发生故障时(如资源交换失败、门户访问异常等),各单位共享交换平台管理员应立即记录故障信息,并将故障具体情况上报共享交换平台管理单位,由管理单位协调运维单位对故障进行定位与排除。

第九十九条 运维单位进行故障处理时,涉及故障的单位须积极配合排除故障。故障排除后,运维单位应做好故障问题分析及处理结果记录,并向管理单位提交故障处理报告。短时间不能排除故障的,运维单位需根据故障等级制定应急方案,并同时向管理单位报备,待管理单位同意后启动应急方案。

第一百条 若共享交换平台运行过程中出现的故障已经严重影响业务正常开展,由管理单位统一部署、安排应急处置工作,各单位按要求积极配合,妥当处理应急处置期间相关业务。管理单位按规定公布故障原因及处理情况,任何人、任何单位未经批准不得擅自披露或散布故障相关信息。

第六节 安全管理

第一百零一条 管理单位牵头、运维单位具体负责建立应急处理和灾难恢复机制,制定事故应急响应和支援处理预案及流程。

第一百零二条 各单位共享交换平台管理员及业务人员应妥善保管用户名及密码,不得转借他人,不得挪作他用,如有丢失,需及时上报管理单位处理。

第一百零三条 各单位应加强共享交换平台使用的内部

管理,确保共享交换平台业务(编目、申请、查询等)正常处理和平台安全稳定运行。

第一百零四条 各单位共享交换平台使用人员应熟练掌握平台的基本操作,及本职工作范围内的平台使用方法。

第一百零五条 运维单位负责共享交换平台病毒防范,在各服务器上安装病毒扫描软件,及时升级杀毒软件,对外部进入的数据应当进行病毒检测。同时,应定期扫描病毒,发现病毒应立即处理。

第一百零六条 因不可抗力造成共享交换平台无法正常运行的,各单位均有义务配合运维单位及时排除故障,并采取补救措施。

第一百零七条 运维单位负责共享交换平台前置库和应用数据库的密码管理、数据备份等工作,并建立完整的服务器、网络等相关技术档案,并定期对服务器、网络等进行巡检。

第一百零八条 所有参与平台开发、管理及运维的人员均需签署信息安全和保密协议,并严格执行国家、省、市及新区保密管理规定,确保操作使用过程中数据的安全性。

第六章 政务服务联动审批系统管理

第一节 系统运行管理

第一百零九条 兰州新区一体化政务服务体系是由新区管委会统一规划建设,为各部门网上政务服务提供公共入口、

公共通道和公共支撑的政务服务一体化平台。

第一百一十条 新区政务服务中心负责一体化政务服务体系应用的组织、协调、指导和督促落实工作。各部门应积极利用电子政务外网和一体化政务服务体系开展工作,并提出进一步完善系统的意见和建议。

第一百一十一条 各部门应接受国家、省、市和新区政务服务体系管理机构的指导、监管,完成纵向业务系统的联通。

第一百一十二条 新区政务服务中心负责一体化政务服务体系有关制度的制定和贯彻落实,组织开展相关政策和系统使用等培训,对一体化政务服务体系规划、建设及发展提出意见需求。

第一百一十三条 新区科技发展局牵头、科技文化旅游集团有限公司负责一体化政务服务体系的建设和运行维护,通过监测、调查、统计等方式,实现提前预警和故障精准处理,通过对监测结果的智能分析与动态可视化,对在线政务服务承载能力进行综合监管。

第一百一十四条 新区科技发展局负责对接入单位的相关服务调整、交更、报备及网络设施等提供第一时间技术支持和便利条件。各接入单位如需改变网络线路,须向新区科技发展局申请许可后方可实施。

第一百一十五条 新区政务服务中心负责统一规划、管理、分配一体化政务服务体系用户权限和账户。因工作需要,

各单位确需增加用户数和用户权限,应向政务服务中心提出书面申请,由系统管理员对入网计算机和用户进行逐个登记,统一分配。经审核符合要求的计算机和用户方可入网运行。

第一百一十六条 各单位每半年应将本单位所有用户及使用者情况上报新区政务服务中心和新区科技发展局登记备案,新区政务服务中心据此对各单位用户使用情况进行清查。

第二节 线上审批业务管理

第一百一十七条 一体化政务服务系统包括如下主要功能:

(一)一窗式业务办理系统:受理群众在政务服务网提交的办理事项,也可在政务大厅现场进行业务办理登记。

(二)电子证照管理系统:实现对各类证照信息的统一规范管理,基于统一的证照资源服务对各业务部门提供证照支撑服务。

(三)电子监察系统:对办件全流程进行监察,生成监察信息,提供预警纠错、督查督办等功能。

(四)电子文件管理系统:将政务服务事项运行过程中产生的电子文件材料统一管理、统一归档,将办件材料电子化,减少纸质材料的提交,实现“一次提交,多处多次复用”。

第一百一十八条 网办优先原则。对公民的政务服务应当逐步向网上办理为主、现场办理为辅过渡;对法人和其他组织的服务要逐步缩减到现场次数,实现绝大部分事项全流程网上办理;对政府部门的服务原则上通过网上办理,直接实现

“一号”申请、“一窗”受理和“一网”通办。

第一百一十九条 电子证照同等效力原则。按照标准规范生成的电子证照,视为满足法律法规规定的原件形式和文件保存要求,与纸质证照具有同等效力,可作为法定依据和归档材料。

第一百二十条 电子证照签发部门应对电子证照的签发、维护、更新、注销工作进行管理,保证证照信息的真实性、完整性、有效性和及时性。

第一百二十一条 符合标准规范的电子证照应在各事项服务主体间互认通行并优先使用;凡通过共享获得业务办理所需电子证照的,各事项服务主体不得要求申请人重复提交该证照的原件、复印件或电子副本,事项办结后可酌情审查原件。证照信息有变更的除外。

第一百二十二条 各部门之间根据职能的合理需要无偿共享信息,法律、行政法规规定不可共享的除外。信息生产和使用部门应当确保信息规范有效、及时、完整、合法、安全,不得擅自隐藏、篡改、隐瞒信息。对无法共享的信息,信息所属部门需提供充分的法律依据,并通过网上政务服务平台告知办事人。

第三节 安全保密管理

第一百二十三条 新区科技发展局牵头、科技文化旅游集团有限公司具体负责,按照国家网络平台安全保障体系相

关标准和网络安全等级保护相关规定,做好一体化政务服务系统的安全建设和安全管控。政务服务中心根据职责做好一体化政务服务系统的帐号、应用等安全监管。

第一百二十四条 各接入单位要建立健全本单位内部安全管理体系,完善管理制度,明确工作职责,确定分管领导和专职管理员落实安全管理责任,并将人员信息报政务服务中心备案。

第一百二十五条 用户应坚持一人一用户原则,计算机用户的使用者在用户登录期间因故离开或者使用结束后必须及时退出系统。

第一百二十六条 严格控制各类用户密码长度(至少 8 位),密码须为“字母+数字”组合;密码不能和用户名相同,也不能使用本人姓名、生日、身份证号码、电话号码等容易被猜出的数字或字母。

第一百二十七条 计算机使用者每三个月必须更改用户密码一次。

第一百二十八条 新区政务服务中心应定期进行检查,对于人员调动未向政务服务中心提出注销用户、私自交接用户和密码的,应对单位负责人及直接责任人予以严肃处理。

第一百二十九条 严禁下列行为,对违反规定造成不良后果的,将依法依规追究相关责任人的责任:

(一)严禁未经允许擅自改变电子政务外网线路;

(二)严禁将一体化政务服务体系用户名、口令转交他人使用；

(三)严禁无关人员登录一体化政务服务体系办理行政审批业务；

(四)严禁盗用他人口令、入侵和破坏一体化政务服务体系；

(五)严禁私自将个人电脑或外部人员电脑接入新区电子政务外网。

第四节 系统维护管理

第一百三十条 新区科技文化旅游集团有限公司按照全国一体化政务服务平台运维管理系统相关标准规范,对网络设备、计算机、存储设备、安全设备等硬件基础设施及操作系统、应用系统、中间件、数据库等软件基础设施的运行状态有效监控和综合管理,实现运维服务流程的标准化,达到一体化平台综合运维要求。

第一百三十一条 为避免计算机病毒传播和网络攻击,保证数据及网络安全,各单位管理员应指导检查本单位计算机安装防病毒软件并及时更新操作系统安全补丁及病毒特征码。所有计算机系统必须定期查杀计算机病毒(每月至少一次)。

第一百三十二条 各单位须做好重要业务系统的数据备份,及时上报运维单位处理网络及系统等故障,对于严重影响政务服务业务办理的同步上报新区政务服务中心和主管部门。

第七章 电子印章应用管理

第一节 电子印章适用范围

第一百三十三条 适用电子印章的文件应是通过网上办公系统流转的各类文件。未经网上办公系统流转的公文及党组文件,暂不适用电子印章。

第一百三十四条 适用电子印章的文件包括:表格类文件、填充类文件、制作类文件(如请示、决定、委托函等)。

第一百三十五条 加盖电子印章的文件与加盖实物印章的纸质文件具有同等法律效力。但该电子文件的复印稿或经任何形式的电子格式转换稿,不具备相同法律效力。

第二节 电子印章的定制和管理

第一百三十六条 各部门根据工作需要确定电子印章的数量,向新区科技发展局提交制章需求,并附电子印章采集表和统一社会信用代码证书,两者信息不一致的必须提供组织部核实证明材料;涉及政务服务事项制作电子印章的需经新区政务服务中心核实确认;党口部门电子印章执行国家和省、市相关规定。新区科技发展局依据采集信息统一制作电子印章印模。

第一百三十七条 各部门电子印章统一配发至办公室负责人或指定专人管理和使用,电子印章专管人员因事、病、休假等原因不在岗位时,应经办公室负责人同意指定他人代管,

并做好交接工作。

第一百三十八条 申请、打印、运行、维护、管理电子印章的工作人员在使用电子印章时要自觉遵守系统运行中相关的规章制度,严格按照权限操作系统和使用电子印章。

第一百三十九条 各单位电子印章管理人员与公章管理人员应当一致,并妥善保管好单位 USBkey 和登陆密码,获取初始密码后应立即修改并定期更换,如忘记密码应报信息技术人员进行处理。如因用户使用初始密码、简单密码或者密码外泄等原因造成不良后果的,将追究管理人员责任。

第三节 电子印章的使用

第一百四十条 电子印章的签署流程与实物印章的加盖流程一致。提起电子印章的文件需按照审批流程通过审批后方可申请加盖电子印章,签章人需审核是否经有签发权人签发后方可使用电子印章。文件、证照未经审批,不能启动电子印章及在线打印程序。

第一百四十一条 文件送审批前,撰稿人或承办人应根据文件性质决定启动电子印章还是传统签章。文件一经使用电子印章,系统自动设定该文件无法编辑。如确需修改,应重新启动审批程序。

第一百四十二条 电子印章管理人要通过信息化应用系统对已经审批的电子文件进行盖章,并定期生成电子印章签章和在线打印情况汇总表,送新区科技发展局统一存档备查。

第一百四十三条 使用电子印章,要做到位置准确,印章端正,清晰,防止错盖、斜盖和模糊。未尽事宜严格执行国家相关法律和《甘肃省一体化在线政务服务平台电子印章管理实施办法(试行)》等规定要求。

第八章 电子证照应用管理

第一节 分 则

第一百四十四条 本细则适用于新区各级行政机关、履行公共管理和服务职能的事业单位以及法律法规授权的其他组织实施电子证照信息采集、制证颁发、归集入库、共享应用、监督管理等相关活动。

第一百四十五条 本细则所称电子证照库,是指由新区统一规划建设,具备电子证照数据归集、存储、查询、核验等功能的管理信息系统。

本细则所称的证照,是指由国家行政管辖范围内各级机关、事业单位和法律法规授权或委托的社会组织颁发的、能够证明资格或权利等凭证类文件。电子证照,是指由计算机等电子设备形成、传输和存储的证件、执照等电子文件。

本细则所称发证单位,是指依据法定职责制作签发电子证照的行政机关、履行公共管理和服务职能的事业单位以及法律法规授权的其他组织。

本细则所称用证单位,是指在依法履职过程中共享使用

电子证照的行政机关、履行公共管理和服务职能的事业单位以及法律法规授权的其他组织。

本细则所称的持证主体,是指电子证照的签发对象,包括自然人、法人和其他组织。

第一百四十六条 电子证照的管理和使用应当遵循以下原则:

(一)标准统一。电子证照的制证签发、数据归集、共享应用等活动应当遵循国家、省、市和新区信息共享管理相关技术与业务标准规范。

(二)同等效力。按照标准规范生成的电子证照与纸质证照具有同等效力,可以作为法定办事依据和归档材料。

(三)实时归集。电子证照应当与实体证照同步生成、发放,实时推送归集。

(四)共享互认。按照标准规范生成的电子证照,在各用证单位之间共享互认。

(五)优先使用。凡可以通过共享获得电子证照的,应当优先使用,不得要求办事企业群众提供实体证照。

(六)安全可控。管理单位、发证单位、用证单位等应当建立健全管理制度和信息安全技术措施,保障电子证照安全可控。

第一百四十七条 新区科技发展局牵头、科技文化旅游集团有限公司具体负责新区电子证照库的建设与维护,承担与全国一体化在线政务服务平台省级电子证照共享服务系统

对接工作、证照数据的信息共享、信息安全等技术保障工作。新区政务服务中心为新区电子证照管理单位,负责统筹规划、协调推进电子证照的管理、应用工作。新区相关部门负责落实推进本系统电子证照管理工作,统筹协调本系统按照新区统一标准制发、归集、应用电子证照。

第二节 制发与归集

第一百四十八条 新区政务服务中心牵头、新区科技展局配合,组织各发证单位编制电子证照目录,明确证照名称、发证单位、证照类型、持证主体、证照模板、照面信息等,并通过新区电子证照库,对目录进行同步更新和维护。

第一百四十九条 发证单位负责本单位电子证照的信息采集、信息审核、制作签发等工作,并对证照信息的完整性、准确性、时效性负责;业务办理中产生的实体证照信息,包括证照的变更、年审、年检、挂失、抵押、暂扣、注销等全过程管理信息,应与电子证照实行同步更新。

第一百五十条 发证单位应把制发电子证照的照面信息、过程管理信息同步归集到新区电子证照库,确保归集入库的数据与证照实际状态一致。

第一百五十一条 除国家另有规定外,发证单位应将有效期内未归集的存量电子证照和有条件实现电子化的历史实体证照信息逐步归集到新区电子证照库。

第一百五十二条 发证单位因不可抗力不能及时制发、

注销、更新电子证照的,应采取应急措施并同步上报管理单位,在故障排除后的3个工作日内完成

第三节 共享与应用

第一百五十三条 用证单位根据政务服务事项办事指南梳理本单位用证清单,并细化应用场景,按照授权共享机制,依法在用证清单范围内应用电子证照。所需电子证照未列入新区政务服务电子证照清单的,应及时向行业部门提出电子证照共享申请,发证单位会同新区政务服务中心、科技发展局归集共享电子证照。

第一百五十四条 新区科技发展局应通过技术手段设置电子证照库的查询、调用权限,确保用证单位在业务范围内规范应用电子证照。用证单位原则上应将本单位业务系统与新区电子证照库对接,通过调用新区电子证照库用证接口的方式,使用、查阅、核验、打印电子证照信息,依法依规应用电子证照。

第一百五十五条 持证主体经过身份认证后,可以通过新区政务服务网或新区“政民通”APP查询其所持电子证照的持证列表、证照详情等信息。

第一百五十六条 用证单位根据持证主体所提供的身份信息,通过政务服务管理平台核验身份信息,并调用与应用场景相关联的电子证照,免提交相应的纸质材料。

第一百五十七条 发证单位、用证单位应将业务办理中

生成和应用的电子证照依法进行电子存档。

第一百五十八条 持证主体对电子证照信息的准确性、完整性和时效性有异议的,可通过政务服务热线提出异议。发证单位收到热线处置工单后 1 个工作日内对相关电子证照进行异议标注,在 5 个工作日内核实情况,并将处理结果告知异议人。

第四节 安全与监督

第一百五十九条 新区科技发展局协同科技文化旅游集团有限公司加强电子证照库的安全基础设施建设,建立电子证照信息安全保障体系,制定应急预案和数据备份恢复制度,确保电子证照信息安全可控。

第一百六十条 发证单位和用证单位应当结合本单位实际,指定专人负责电子证照管理工作。

第一百六十一条 发证单位和用证单位应加强本单位业务系统和电子证照的信息安全管理,保障电子证照信息合法合规使用,并保护持证主体的商业秘密和个人隐私。

第一百六十二条 发证单位和用证单位应结合本单位工作实际,优化业务流程、完善办事指南,消除电子证照推广应用的制度障碍。

第一百六十三条 新区政务服务中心应会同新区科技发展局通过随机抽查、模拟办事、电子督查等方式对各部门发证单位和用证单位的电子证照归集和应用情况进行日常督查,

督促发证单位持续提高数据归集的及时性、完整性和准确性，持续提高用证单位电子证照的适用率、应用率和成功率。

第九章 网络与政务数据安全应急预案

第一节 分 则

第一百六十四条 为规范兰州新区网络与政务数据安全重大事件报告管理工作，及时掌握和评估网络与数据安全重大事件有关情况，协调组织技术力量进行事件的应急响应处理，有效预防、及时控制和最大限度地降低网络与数据安全重大事件所造成的损失和影响。根据《中华人民共和国计算机数据安全保护条例》《中华人民共和国突发事件应对法》《中共中央办公厅、国务院办公厅转发〈国家信息化领导小组关于加强网络与数据安全保障工作的意见〉的通知》等法律法规规定，结合新区实际，制定本预案。

第一百六十五条 本预案所称网络与数据安全重大事件是指因自然灾害、人为攻击或破坏以及病毒爆发、网上泄密、设备故障等原因所引发，严重影响新区网络正常运行，造成业务中断、系统瘫痪、数据破坏或信息泄密等，从而在政府形象、社会稳定或公众利益等方面造成严重影响以及一定程度直接和间接重大经济损失的事件。

第二节 事件类别及级别划分

第一百六十六条 网络与数据安全突发事件的类别、级别。

（一）突发事件的类别。

根据网络与数据安全的发生原因、性质和机理，兰州新区网络与数据安全主要分为以下四类：

1. 网上泄密事件：指在兰州新区网络环境发布了涉及国家秘密、商业秘密、内部资料、个人隐私等不允许公开的信息。

2. 攻击类事件：指网络系统因计算机病毒感染、非法入侵等导致业务中断、系统死机、网络瘫痪等情况。

3. 故障类事件：指网络系统因计算机软硬件故障、人为错误操作等导致业务中断、系统死机、网络瘫痪等情况。

4. 灾害类事件：指因爆炸、火灾、渗水、雷击、地震、风暴等外力因素导致网络系统损毁，造成业务中断、系统死机、网络瘫痪等情况。

（二）突发事件的级别。

数据安全事件分级的参考要素包括数据密级、公众影响、业务影响和财产损失等四项。各参考要素分别说明如下：

1. 数据密级是衡量因数据失窃或泄密所造成的数据安全事件中所涉及信息重要程度的要素。

2. 公众影响是衡量数据安全事件所造成负面影响范围和程度的要素。

3. 业务影响是衡量数据安全事件对事发单位正常业务开展所造成负面影响程度的要素。

4. 财产损失是衡量恢复系统正常运行和消除数据安全事

件负面影响所需付出资金代价的要素。数据安全突发事件级别分为四级：一般（IV级）、较大（III级）、重大（II级）和特别重大（I级）。

IV级：新区内较大范围出现并可能造成较大损害的数据安全事件。

III级：新区重要部门网络与信息系统、重点网站或关系到本地区社会事务或经济运行的其他网络与信息系统受到大面积严重冲击。

II级：新区重要部门或局部基础网络、重要信息系统、重点网站瘫痪，导致业务中断，纵向或横向延伸可能造成严重影响或较大经济损失。

I级：敌对分子利用信息网络进行有组织大规模的宣传、煽动和渗透活动，或者新区各部门多地点或多个基础网络、重要信息系统、重点网站瘫痪，导致业务中断，造成或可能造成严重影响或巨大经济损失的数据安全事件。

第三节 处置流程

第一百六十七条 应急处理组织机构由新区党工委办公室、管委会办公室、公安局、应急管理局、科技发展局、电信分公司、移动分公司、联通分公司和各电子政务外网使用单位组成，负责网络与数据安全应急处理。新区政务网络环境日常工作由党工委办公室协调运行，特殊情况下，事故涉及的相关单位要予以配合协助。

第一百六十八条 出现应急事件后值班人员要及时通过电话、短信等方式通知单位领导及相关技术负责人。值班人员根据灾情信息,初步判定灾情程度。能够自身解决的,要及时加以解决;不能自行解决的,由单位领导现场指挥,协调各部门力量,按照分工负责的原则,组织相关技术人员进行应急处理。

(一)病毒爆发处理流程

各单位对外服务信息系统一旦发现感染病毒,应执行以下应急处理流程:

1. 立即切断感染病毒计算机与网络的联接。
2. 对该计算机的重要数据进行数据备份。
3. 启用防病毒软件对该计算机进行杀毒处理,同时通过防病毒软件对其他计算机进行病毒扫描和清除。
4. 如果满足下列情况之一的,应立即向本单位数据安全负责人通报情况,并向党工委办公室报告:
 - (1)现行防病毒软件无法清除该病毒的;
 - (2)网站在 2 小时内无法处理完毕的;
 - (3)业务系统或办公系统在 4 小时内无法处理完毕的。
5. 恢复系统和相关数据,检查数据的完整性。
6. 病毒爆发事件处理完毕,将计算机重新接入网络。
7. 总结事件处理情况,并提出防范病毒再度爆发的解决方案。

8. 实施必要的安全加固。

(二) 网页非法篡改处理流程

各单位对外服务网站一旦发现网页被非法篡改,应执行以下应急处理流程:

1. 发现网站网页出现非法信息时,值班人员应立即向本单位数据安全负责人通报情况,并立即向新区公安局和党工委办公室报告。情况紧急的,应及时采取断网等处理措施,再按程序报告。

2. 本单位数据安全负责人应在接到通知后立即赶到现场,做好必要记录,妥善保存有关记录及日志或审计记录。

3. 协调公安机关赶到现场,追查非法信息来源。新区党工委办公室和科技发展局做好相关配合工作,必要时协调相关部门或运营商配合处理。

4. 在新区公安局提取相关数据样本后,清理网站非法信息,强化安全防范措施,然后将网站重新投入使用。如情节严重,构成犯罪的,由公安局立案侦查。

5. 总结事件处理情况,并按照事件严重程度逐级汇报,新区党工委办公室对处理情况进行备案。

6. 实施必要的安全加固。

(三) 非法入侵处理流程

一旦发现信息系统存在被远程控制等非法入侵行为,应执行以下应急处理流程:

1. 发现系统服务器被远程控制、植入后门程序,或发现有黑客进行攻击时,应立即向党工委办公室报告,并立即向公安局通报。

2. 如服务器已被入侵,将被攻击的服务器等设备从网络中隔离出来,保护现场。

3. 本单位数据安全负责人应在接到通知后立即赶到现场,做好必要记录,妥善保存有关记录及日志或审计记录。

4. 通知新区公安局赶到现场采样,对现场进行分析,追查攻击源,指导主管部门修改防火墙等设备的安全配置阻断黑客继续入侵,必要时协调相关部门或运营商配合处理。

5. 分析后台数据库操作日志,判断是否发生数据失窃。检查、校验数据的完整性和有效性。

6. 在新区公安局提取相关数据样本后,恢复与重建被攻击或破坏的系统。如情节严重,构成犯罪的,由新区公安局立案侦查。

7. 总结事件处理情况,并按照事件严重程度逐级汇报,新区党工委办公室对处理情况进行备案。

8. 实施必要的安全加固。

(四) 网上泄密事件应急处理流程

一旦发现网上有涉密信息,应执行以下应急处理流程:

1. 发现电子政务外网上存在涉密信息时,应立即切断网络连接,并向本单位数据安全负责人通报情况,查找泄密来

源,并立即向新区党工委办公室报告。

2. 本单位数据安全负责人应在接到通知后立即安排管理人员删除所发布的涉密信息,对涉密信息的扩散情况进行追查,并全面删除。

3. 新区党工委办公室负责对网上涉密信息进行密级鉴定并指导做好补救措施。组织协调有关部门对计算机网络上泄露秘密的行为进行查处。

4. 总结事件处理情况,并按事件严重程度逐级汇报,新区党工委办公室对处理情况进行备案。

(五)机房物理环境事故应急处理流程

1. 供电故障:如果出现短路、断路及防雷防静电设备故障,应立即切断电源,并及时维修或更换损坏设备,确保最短时间内恢复供电;新区电力部门办理线路维修或其他停电业务时,要及时通知新区党工委办公室,若停电超过2小时的,由电力部门提供应急发电车配合供电。

2. 火灾事故:如发生火灾,应立即切断电源,并用灭火器灭火。向119指挥中心报告火警,请求支援,如有人员遇险,应先救人后救物。

3. 渗水故障:如出现渗水故障,应立即切断电源,及时更换浸水设备并采取防渗水措施。

(六)网络线路故障应急处理流程

1. 电子政务外网网络故障:如发生链路、网络设备故障等

情况时,由运维技术人员及时采取相应技术措施保障网络畅通。对需要抢修的线路,如果属于自建链路,运维人员应立即赶赴现场抢修;如租用其它电信运营商的链路,通知相关运营商及时抢修,若链路无法修复,运营商应协调架设临时链路,或提出其他解决方案。

2. 网络及安全设备故障:对所有网络设备进行实时监测,值班人员一旦发现异常,应立即向新区党工委办公室相关负责人报告,经现场检测抢修后,若问题较严重的,及时上报情况。同时,主管部门组织相关技术人员进行应急维修,对一时无法修复的,需立即借用或紧急采购新设备进行更换。对已达到报废年限但未损坏的设备,要随时准备好备品备件。

(七)数据故障应急处理流程

服务器或存储设备故障:机房所有重要数据应采取异地备份或人工备份,若发生故障时,要保护好存储磁盘数据安全,及时组织技术人员对故障点进行排查,设备恢复正常后,及时恢复相关数据;若出现重大故障,原设备数据无法恢复的,在更换新设备后,要及时恢复异地备份或人工备份数据,保证系统在最短时间内能够正常运行;故障处理完毕后,要在2个工作日内整理分析造成事故的原因,针对具体问题,采取相应安全措施并报新区党工委办公室备案。

(八)设备防盗被盗或人为损害应急处理流程

1. 发生设备被盗或人为损害设备情况时,运维值班人员

应立即报告新区主管部门相关负责人,同时保护好现场。

2. 立即通知保安及公安部门,一同核实审定现场情况,清点被盗物资或盘查人为损害情况,做好必要的影像记录和文字记录。

3. 积极配合公安部门进行调查,并将有关情况向上级主管部门汇报。

第一百六十九条 机房发生突发事件后,主管部门应采取有效措施开展先期处置,恢复信息网络正常状态。应急处置工作结束后,应对事件发生原因、性质、影响、后果、责任及应急处置能力、恢复重建等问题进行全面调查评估,根据应急处置中暴露出的管理、协调和技术问题,改进和完善预案,实施针对性演练,总结经验教训,整改存在隐患,组织恢复正常工作秩序。

第十章 附 则

第一百七十条 本办法由兰州新区科技发展局负责解释。

第一百七十一条 本办法适用于兰州新区各园区管委会,各部门、各单位,新区各国营集团公司,省属驻区各单位、各镇党委和人民政府及监管国有企业。

第一百七十二条 本办法自印发之日起施行,有效期2年。

电子印章印模采集表

填表日期： 年 月 日

使用单位	统一社会信用代码		行政区划代码	
	单位名称			
	详细地址			
经办人信息	姓名		身份证号	
	职务		电话	
法人信息	姓名		身份证号	
	职务		电话	
用途描述（证照名、或其他）			印章尺寸（直径）	cm
实体印章要求 （油印均匀，图像无重影，每枚印章采集二个样本）	盖章1		盖章2	
电子印章 领取声明	自电子印章管理员领取电子印章之日起，该电子印章的授权管理由该管理员负责。			

- 要求：1、盖章时请务必用力按压，保证印章字迹清晰可辨，盖到空白处，不要压线；
- 2、同一个印章应该盖两次；
- 3、扫描成电子格式时分辨率不低于300dpi。

兰州新区管委会办公室

2021 年 9 月 14 日印发

共印 15 份