岚县社会信用体系建设工作领导小组办公室文件

岚信用办发〔2021〕8号

岚县公共信用信息平台
数据安全保护和应对管理制度

第一章总则

第一条为加强和规范岚县信用信息共享平台及信用门户网站(以下简称“信用岚县”)的安全管理工作，结合信用平台建设情况及应用特点，切实保护法人和自然人的合法权益，根据《中华人民共和国计算机信息系统安全保护条例》、 《中华人民共和国民法典》、国务院《社会信用体系建设规划纲要(2014-2020年)》 (国发〔2014〕21号)、《国务院办公厅关于进一步完善失信约束制度构建诚信建设长效机制的指导意见》国办发〔2020〕49号等文件要求，

结合工作实际，特制定本制度。

第二条“信用岚县”是指基于岚县电子政务外网和岚县电子政务公共服务云平台，由计算机硬件、网络和安全设备、计算机软件、业务应用系统及其相关的配套设施等构成，按照一定的应用目的和规则对公共信用信息进行征集、清洗、比对、分析、共享等处理的信息系统。

第三条本制度所称数据安全保护和应对管理内容包括：安全管理组织机构、人员管理、安全建设管理、安全运行管理、应急预案、数据安全及个人隐私保护等方面。

第四条信用岚县数据安全保护和应对管理工作坚持“预防为主、主动防御、综合防范”的指导方针，采取技术与管理相结合的措施，重点保障基础网络和重要信息安全，全面提高信用平台安全防护能力，并按照国家有关规定实行等级保护，建立安全保障体系。

第五条本办法适用于建设、运行、维护、管理和使用信用岚县的各级政府部门、金融机构、公共服务单位及其工作人员。

第六条任何参与信用岚县开发建设、运营维护、公务使用的各级政务部门和公共服务企事业单位，不得利用职务之便从事危害国家利益、集体利益的活动，不得侵害市场主体和自然人的合法权益，不得危害信用岚县的安全。

第二章安全管理组织机构

第七条为加强信用平台信息安全组织领导，明确责任，落实任务，增强责任心和工作主动性，设立信用平台信息安

全领导小组(以下简称“领导小组”),成员由岚县信用体系建设联合单位有关人员组成；领导小组办公室设在岚县发展和改革局。

第八条领导小组及其办公室(以下简称领导小组办公室)作为全县信用体系建设的主管机构，承担如下职责：

(一)统筹协调全县社会信用体系建设工作，组织推进社会信用体系建设各专项工作的开展，组织开展国家、省、市社会信用体系建设示范试点工作开展；

(二)根据国家有关信息安全政策、法律法规等文件要求，制定和印发信用岚县标准规范、管理制度、安全策略、实施方案等。

(三)根据信用岚县的基本规范和管理办法，监督安全措施的执行，督促、检查各成员单位落实情况，协调解决涉及信用平台安全的重大问题及突发事件。

(四)对信用岚县的建设、运行、维护、管理和使用进行具体指导；建立调度或考核机制，及时调度分析，督促各级各部门及时归集公示和查询使用公共信用信息。

(五)全面推进信用岚县应用的建设及开展，切实将公共信用信息归集公示和查询使用的工作部署，落实到社会信用体系建设的各个环节、各个领域，确保全覆盖、无遗漏。

(六)组织开展信用体系建设、岚县信用信息共享平台及信用门户网站使用相关业务培训。

第九条其他使用信用岚县的各级政务部门和公共服务企事业单位及机构，应当在按照国家法律、法规和有关规定

建立健全本部门、单位数据安全管理制度和工作规范，保障信用岚县数据安全的前提外之外，承担如下职责：

(一)做好公共信用信息的归集、上报工作，做到“应归尽归”；

(二)在依法依规的前提下，全面推进和落实信用信息在各个环节、各个领域、各行业的信用应用；

(三)县级信用体系主管单位应建立“信用中国(吕梁岚县)”网站的信息内容更新保障机制，及时发布信用体系建设相关的重要会议、重要活动、重大政策信息，做到决策公开、执行公开、管理公开、服务公开、结果公开；

(四)网站管理、审核单位应做好网站信息的采编、维护工作，突出重点、放大亮点，严格采集、审核、报送等程序，尤其要对涉及歪曲党史、国史和带有暴力、色情、反动内容的信息进行清查和甄别，保证所维护的信息内容合法、完整、准确、及时，并做好公开属性和保密审查；

(五)县级各信源单位需严格按照网站动态信息标准(包括动态信息标题、动态信息链接地址、本单位领导审核意见、动态信息发布栏目、动态信息采编时间)进行动态信息的上报；若上报动态信息为文字材料，需通过邮箱、考盘等方式及时上报；

(六)与信用岚县开展数据交换或系统对接的各级部门，负责组织本部门信息系统安全建设，确保交换信息和接入系统的安全运行。

第三章人员管理

第十条各单位应当对涉及信用岚县系统及数据资源的相关人员进行必要的风险防控措施，选派业务能力强的人员从事信用信息工作，最大程度降低由人员本身导致的数据安全风险。人员定岗时应签署保密协议；人员离岗时应规范人员离岗过程，办理严格的调离手续，所在主管单位应将本人的账号信息报送县发展改革局进行注销，将所接触或掌握的信用信息进行专项交接；加强各类人员的安全意识教育和培训等。

第十一条系统开发、管理维护、使用人员应当严格按照信用岚县操作权限和岗位职责操作和使用系统，不得将本人账号、密码及所掌握和查询到的信息转予他人使用明确信息查询使用的权限和程序，不得将公共信用信息泄露给与工作无关的第三方，对故意或因工作失误泄露信息的，要依法依规严格追究相关单位和人员责任。

第十二条网络管理员负责信用岚县承载网络岚县电子政务公共服务云平台的网络安全管理和日常运行维护的网络安全，并负责岚县电子政务外网的网络安全管理和日常运行维护的网络安全管理。

(一)负责信用岚县承载网络的规划与部署，确保网络畅通，掌握各信息结点、各类网络设备的通断情况，以及网络地址和端口的分配、设置和规划。

(二)负责网络设备和安全设备的配置与管理，负责设备的正常启动与关闭。

(三)每天定时查看网络设备和安全设备运行日志，了解承载网络运行状况，在网络及设备异常或故障发生时，及时分析原因并进行处理，消除故障隐患，填写《设备故障处理记录表》,并及时上报。

(四)每月对网络主要硬件设备进行检查与维护。

(五)负责对关键网络配置文件进行备份，及时修补网络设备的漏洞。

(六)协助安全管理员制定网络设备安全配置规则，并落实执行。

(七)为安全审计员提供完整、准确的重要网络设备运行活动的日志记录。

(八)编制网络设备的维修、报损、报废等计划。

第十三条数据库管理员，全面负责数据库系统的管理工作，保证其安全、可靠、正常运行。做好数据库服务器的运行记录，当数据库服务器出现故障时，迅速会同相关人员一同解决。

(一)负责数据库系统的建设，做好数据库服务器的维护、数据库软件的安装、卸载、升级、备份和日志等工作。

(二)具体负责数据库维护管理任务，解决应用系统数据库方面问题，分析定位数据库故障，确定数据库问题的临时和永久解决方法，跟踪整个检修过程。

(三)参与数据安全应对制度的制定、测试、演练，制定备份与恢复策略，定期在测试环境中进行恢复方案的模拟测试，检查数据恢复是否成功。识别数据库环境的定时任务

需求，参与定时任务的定制和测试任务。识别数据库性能和容量的需求，根据性能建议调整数据库容量和其他数据库性能配置。制定数据库的性能报告，评审数据库性能报告，识别趋势并提供改进建议。

（四）根据应用系统的需求创建数据库表、索引，修改数据库结构等。对数据库版本进行管理，提出版本升级计划，需要时安装数据库系统补丁，并做好记录。

（五）监测有关数据库的告警，检查并分析数据库系统日志，及时提出解决方案，并记录服务支撑日志。定期检查数据库资源联通性、自动备份情况、定期修改情况。

（六）按规定授权原则确定不同用户的数据访问权限。按照用户类别和权限，使数据的使用被限制在工作确需的范围内。规定数据类别、用户使用的许可等级和相应的数据使用规则，以保证数据的安全使用。明确处理数据的范围、权限、级别，并能防止越权操作。

第四章安全建设管理

第十四条物理安全策略

（一）信用平台设在在岚县发展和改革局机房，该中心选择在具有防震、防风和防雨等能力的建筑内，避免设在建筑物的高层或地下室。

（二）机房出入口安排专人值守，重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。

（三）需进入机房的来访人员经过申请和审批流程，并限制和监控其活动范围。

(四)对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域。

(五)机房内部署基础防护系统和设备，如防盗、温控制和UPS 供电系统。

第十五条网络安全策略

(一)保证主要网络设备的业务处理能力具备冗余空间，保证网络各个部分的带宽，以满足信用平台业务高峰期需要。

(二)根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段。

(三)应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段。

(四)应在网络边界部署访问控制设备，根据实际安全需求设置访问控制策略启用访问控制功能。

(五)对网络系统中的网络设备运行状况、网络流量、用户行为等进行审计，并对审计记录数据进行分析，生成审计报表，且保护审计数据。

(六)能够对非授权联接行为进行检查，准确定出位置，并对其进行有效阻断。

(七)在网络边界处监视攻击行为，记录发生的攻击行为。

(八)在网络边界处监视，并维护恶意代码库的升级和

检测系统的更新。

(九)对登录网络设备的用户进行身份标识和鉴别，并设置身份标识和鉴别方式，字母和特殊字符相结合的方式，且不少于10位。

第十六条主机安全策略

(一)对登录操作系统和数据库系统的用户进行身份标识和鉴别，并设置身份标识和鉴别方式，字母和特殊字符相结合的方式，且不少于10位。

(二)启用访问控制功能，设置访问控制策略，依据安全策略控制用户对资源的访问。

(三)对服务器和重要客户端的重要用户行为、系统资源的异常使用和重要系统命令的使用等内容进行安全审计，并对审计记录数据进行分析，且保护审计数据。

(四)确保操作系统和数据库系统用户的鉴别信息，系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

(五)能够对重要服务器进行入侵的行为和对重要程序的完整性进行检测。

(六)安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库，并支持防恶意代码的统一管理。

第十七条应用安全策略

(一)提供专用的登录控制模块对登录用户进行身份标识和鉴别，并设置身份标识和鉴别方式。

(二)提供访问控制功能，依据安全策略控制用户对文

件、数据库表等客体的访问。

(三)确保应用系统用户的鉴别信息，系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。

(四)具有在请求的情况下为数据原发者或接收者提供数据原发、接收证据的功能。

(五)应用系统须具有软件容错功能，提供数据有效性检验功能和自动保护功能。

第十八条数据安全策略

(一)能够检测到信用平台管理数据、鉴别信息和重要业务数据在传输和存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

(二)采用加密或其他有效措施实现信用平台管理数据、鉴别信息和重要业务数据传输和存储保密性。

(三)应提供本地数据备份与恢复功能，完全数据备份至少每周一次，备份介质场外存放。

第十九条系统建设管理策略

(一)明确信用平台的边界和安全保护等级，并组织相关部门和有关安全技术专家对信用平台定级结果的合理性和正确性进行论证和审定。

(二)根据信用平台的等级划分情况，统一考虑安全保障体系的总体安全策略、安全技术框架、安全管理策略、总体建设规划和详细设计方案，并形成配套文件。

(三)制定详细的工程实施方案控制实施过程，并要求

工程实施单位能正式地执行安全工程过程。

(四)在测试验收前根据设计方案或合同要求等制订测试验收方案，在测试验收过程中应详细记录测试验收结果，并形成测试验收报告。

(五)信用平台相关备案材料报公安机关备案。

(六)每年对信用平台进行一次等级测评，发现不符合相应等级保护标准要求的及时整改。

第五章安全运行管理

第二十条信用岚县配合县发展和改革局加强对服务器、网络设备等硬件设施的使用、维护、管理，防止外来硬件设备擅自接入，防止私自拆卸、添加或销毁硬件设备，防止服务器及网络设备私自带离机房。

(一)机房基础设施指岚县物理机房设备为信用平台提供运行保障和运行环境的场地设施。包括容纳信用平台的机房、支持信用平台运行的供电系统(含UPS 系统)等配套设施。

(二)对机房关键基础设施设备的重大维修、安装操作，应事先制定标准维护流程。可要求外部技术支持公司提供制定标准维护流程的标准和操作建议，机房管理人员负责最终确认审核，并由机房管理负责人批准实施。

(三)应定期对基础设施设备运行情况进行巡检。每日巡检由机房管理人员完成，每月巡检和每季巡检由外部技术支持公司和机房管理人员共同完成，重点排查基础设施设备运行隐患、解决遗留问题、定期完成设备部件更换等。

(四)信用岚县承载网络在建设前应充分论证、详细设计， 一旦正式投产使用，不得随意修改其结构和参数。已投产的网络系统因业务发展或其它原因确需进行结构及参数调整的，应严格执行网络变更流程。

(五)网络IP地址应统一规划，未经允许，不得私自设置和更改IP地址。

(六)应定期整理信用平台承载网络的拓扑结构、配置参数、地址等资料，发生变更时应及时更新。

(七)应实现网络和安全设备的最小服务配置，应对网络和安全设备的配置文件进行定期离线备份。

(八)应启用网络设备和安全设备的日志功能，防火墙、入侵检测系统和路由器等系统日志的保存期限至少一年。

(九)应每日对主干网络进行巡检，测试网络连通性，及时发现网络的连通故障。

(十)应每日检查硬件日志，对网络流量和网络性能进行监控、分析和管理。

(十一)出现故障时，系统管理员应在第一时间内排除故障，以保证网络的连续正常运行。

第二十一条账号管理

(一)信用平台所有账号(包括业务应用系统、网络设备、安全设备、服务器、存储和终端计算机的账号)的申请应遵循以下原则：任何系统的账号必须按照规定的流程进行；账号相应的权限应该以满足用户需要为原则，不得有与用户职责无关的权限。

(二)系统应当严格限制开设公用账号，　一般情况下公用账号不得具有访问敏感信息和对系统写的权限。

第二十二条系统变更管理

(一)信用平台工作人员根据业务需要，提出变更设备或者系统的申请，应提交设备和系统变更申请报告，说明变更原因、效果和影响，变更时间和费用，实施方案(包括变更失败的应急措施)等内容。

(二)县信用办对变更申请进行审批，确保变更的必要性，评估对业务的影响，决定是否批准变更。

(三)对设备或系统进行测试和变更时，尽量在非业务时间，减少对信用平台正常业务的干扰。在变更失败时，能顺利切换原有系统。

(四)县信用办对变更实施进行验收，验证通过则变更完成。验证未通过则重新提交变更方案。

(五)变更完成后，将变更信息及时通知给相关部门、人员。

(六)进行设备和操作系统的变更时，系统管理员应该把成功的或者不成功的变更以及未预料事件做出记录，最后归档。

第二十三条信源单位应加强对接入信用岚县的各终端计算机的安全检查，各终端计算机必须安装使用防病毒和防火墙软件，并定期更新升级，及时进行木马程序和病毒代码全面扫描，定期进行系统漏洞扫描，对发现的系统安全漏洞及时修补。

第六章应急预案

第二十四条岚县发展和改革局负责建立健全信用岚县信息安全应急响应机制，科学应对平台与公共信用信息安全突发事件，有效预防、及时控制、最大限度消除各类突发事件的危害和影响。

第二十五条本预案适用于我县范围内发生的严重影响网络与平台正常运行的网络与信息事件，造成系统中断、系统破坏、数据破坏或公共信用信息被窃取、泄露，侵害市场主体和自然人合法权益，造成社会不良影响和经济损害。

第二十六条网络与信息事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障和灾害性事件等。有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件；网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件；信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件；信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件；设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障；灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

第二十七条网络与信息安全事件分为四级： Ⅰ级(特别重大网络与信息安全事件)、Ⅱ级(重大网络与信息安全事件)、Ⅲ级(较大网络与信息安全事件)、 Ⅳ级(一般网络与信息安全事件)。

第二十八条符合下列情形之一的，为特别重大网络与信息安全事件(Ⅰ 级):信息系统中断运行48小时以上；平台数据丢失或被窃取、篡改、虚构、违规删除信用信息超过5万条，对市场主体和自然人构成特别严重损害；泄露涉及国家秘密、商业秘密、个人隐私的市场信用信息超过5万条；未经信用主体授权擅自将非公开的市场信用信息提供给第三方查询或者使用超过5万条；其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络与信息安全事件。

第二十九条符合下列情形之一且未达到特别重大网络与信息安全事件(Ⅰ 级)的，为重大网络与信息安全事件(Ⅱ级):信息系统中断运行24小时以上；平台数据丢失或被窃取、篡改、虚构、违规删除信用信息超过2万条，对市场主体和自然人构成特别严重损害；泄露涉及国家秘密、商业秘密、个人隐私的市场信用信息超过2万条；未经信用主体授权擅自将非公开的市场信用信息提供给第三方查询或者使用超过2万条；其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络与信息安全事件。

第三十条符合下列情形之一且未达到重大网络与信息

安全事件(II级)的，为较大网络与信息安全事件(III级)：信息系统中断运行12小时以上；平台数据丢失或被窃取、篡改、虚构、违规删除信用信息超过1万条，对市场主体和自然人构成特别严重损害；泄露涉及国家秘密、商业秘密、个人隐私的市场信用信息超过1万条；未经信用主体授权擅自将非公开的市场信用信息提供给第三方查询或者使用超过1万条；其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络与信息安全事件。

第三十一条除上述情形外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络与信息安全事件，为一般网络与信息安全事件（IV 级）

第三十二条网络与信息安全事件预警等级分为三级： I级(特别重大)、II级(重大)、III级(较大),依次用红色、橙色和黄色表示，分别对应发生或可能发生特别重大、重大和较大的网络与信息安全事件。

第三十三条各级政务部门和公共服务企事业单位都有义务向县信用办报告网络与信息安全事件及其隐患。网络与信息安全事件发生后，相关政务部门和公共服务企事业单位在做好先期处置的同时注意保存证据，会同县信用办立即组织研判，提出预警等级建议。 I级(特别重大)、II级(重大)网络与信息安全事件，要在1小时内上报县政府。III级(较大)、 IV级(一般)网络与信息安全事件，要在2小时内上报县政府。

第三十四条 IV 级(一般)网络与信息安全事件由相关部门或单位进行调查处理和总结评估。对事件的起因、性质、影响、责任等进行调查，并提出处理意见和改进措施。调查处理和总结评估工作原则上在应急响应结束后30天内完成，上报县信用办。 I 级(特别重大)、II级(重大)、III级(较大)网络与信息安全事件由县信用办配合县政府和有关部门进行调查处理和总结评估。

第三十五条各级政务部门和公共服务企事业单位应当加强突发网络与信息安全事件预防和处置的有关法律、法规和政策的宣传，开展网络与信息安全基本知识和技能的宣讲活动，提高防范意识及技能。

第七章数据安全及个人隐私保护

第三十六条各信源单位应加强对公共信用信息的安全管理和保存，杜绝泄密和失密情况发生，公共信用信息包含信用岚县归集、共享的各类信息及“信用中国(吕梁岚县)”网站上的信用动态、政策法规等栏目下维护的相关图片、视频以及文字信息等。各单位应积极制定信用信息数据安全管理措施，确保工作流程不泄密、传输过程不失密和安全存档防窃密。

第三十七条信用岚县的各类信用记录、统计分析报告等信用成果和信用数据的共享、开放权限，由县发展和改革局统一设置、统一审批，并按相关要求与信源单位签订使用协议，任何单位或个人未经批准不得使用或向第三方提供信用成果和数据。

第三十八条各信源单位应加强信用信息存储介质的管理，确保存储介质登记造册、安全使用、分级存放，防止敏感、涉密数据信息泄露；对需要送修和销毁的存储介质，要确保存储内容清除和不可恢复。

第三十九条各级政务部门和公共服务企事业单位及机构应当遵循合法、正当、必要、最小化原则，严格按照公共信用信息目录收集使用个人信用信息，明示收集使用信息的目的、方式和范围并经本人同意，法律、法规另有规定的从其规定。禁止任何单位和个人未经授权、强制授权或一次授权终身收集使用个人信用信息。加大对非法获取、传播、利用以及泄露、篡改、毁损、窃取、出售个人信息等行为的查处力度。相关部门要对金融机构、征信机构、互联网企业、大数据企业、移动应用程序运营企业实施重点监管，严格规范其收集、存储、使用、加工、传输、提供和公开个人信息等行为。

第八章附则

第四十条本办法由岚县发展和改革局负责解释。

第四十一条本办法自发布之日起实施，未尽事宜以国家相关安全规范为准。

（此文主动公开）

岚县社会信用体系建设领导小组办公室

2021年5月30日

岚县社会信用体系建设领导小组办公室　　2021年5月30日印发