黑河市诚信黑河建设工作领导小组办公室

黑市诚信办发〔2020〕20号

关于印发《黑河市信用信息共享平台数据安全保护和应对制度》的通知

市“诚信黑河”建设工作领导小组各成员单位，各县（市、区）：

为贯彻落实信息安全管理有关规定，加强和规范黑河市信用信息共享平台的安全管理工作，切实保护法人、自然人的合法权益，维护网络运行安全，特制定《黑河市信用信息共享平台安全管理暂行办法》等制度，现将通知印发给你们，请严格遵守相关制度。

附件：1.《黑河市信用信息共享平台安全管理暂行办法》

2.《黑河市信用信息共享平台信息安全组织及职责管理规定》

3.《黑河市信用信息共享平台内、外部人员安全管理规定》

4.《黑河市信用信息共享平台安全审核和安全检查制度》

市“诚信黑河”建设工作领导小组办公室

2020年12月22日

附件 1：

黑河市信用信息共享平台安全管理暂行办法

第一章　总则

第一条　为加强和规范黑河市信用信息共享平台（以下简称“市信用平台”）安全管理，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》（国务院令第 147 号）、国务院《社会信用体系建设规划纲要（2014—2020 年）》（国发〔2014〕21 号）及有关法律、法规，结合工作实际，制定本办法。

第二条　本办法所称市信用平台安全管理，是指在市信用平台立项、建设、运行、维护、管理及废止等过程中保障信用信息及其相关系统、环境、网络和操作安全的一系列管理活动。市信用平台包括黑河市信用信息共享平台、“信用黑河”网站、微信公众号。

第三条　本办法适用于建设、运行、维护、管理、使用市信用平台的各级各部门、金融机构、公共服务单位及其工作人员。

第二章　安全管理职责

第四条　黑河市“诚信黑河”建设工作领导小组办公室（以下简称“市信用办”）作为市信用平台主管部门和管理机构，承担以下安全管理职责：

（一）制定市信用平台安全管理的总体策略、基本规范和制度；

（二）制定市信用平台安全管理技术标准和具体保障措施；

（三）负责市信用平台重大信息安全事件的查处和通报；

（四）负责市信用平台建设、运行、维护和日常安全管理及技术保障工作；

（五）检查、督促、指导市信用平台使用单位的安全管理工作，定期开展评价和通报；

（六）督导市信用平台用户单位严格落实各项安全管理制度；

（七）组织市信用平台用户单位安全管理培训；

（八）及时收集、分析、上报市信用平台安全管理工作的基本情况，提出工作意见和建议。

第五条　各级各部门、信用服务机构、金融机构、公共服务单位作为市信用平台用户单位，承担以下安全管理职责：

（一）根据市信用平台安全管理制度，落实本单位使用市信用平台的安全管理措施；

（二）与市信用平台存在数据交换的用户单位，按照市信用平台总体安全策略，配备技术设备和人力资源，确保数据交换设备和接入系统的安全运行。

第三章　人员管理

第六条　市信用平台工作人员，主要包括市信用平台的开发人员、管理维护人员及使用人员(以上人员简称“系统工作人员”)。系统工作人员应自觉遵守有关法律法规和内部制度，接受保密教育和监督，维护公共信用信息及相关资料档案的安全。

第七条　系统工作人员上岗前，须参加公共信用信息安全培训，并与单位签订保密协议，承担保密责任,履行保密义务。

第八条　系统工作人员应当严格按照内部制度、岗位职责和操作权限进行系统操作，不得将操作账号或 CA 介质转予他人使用，不得通过电话、拍照、网络、邮件等任何方式将公共信用信息泄露给与具体工作无关的第三方。

第九条　系统工作人员办理转岗或离职手续时,应将所接触或掌握的保密信息,向市信用办指定人员或部门作专项交接,并按照保密协议规定严格履行保密义务。

第四章　信息载体及运行维护管理

第十条　保密信息载体是指存储公共信用信息、内部资料以及重要公文等材料的硬盘、软盘、U 盘、磁盘及缩微胶片等载体。

第十一条　信息载体实行专人管理、分级存放，其发放、使用、更换和销毁等均须履行登记签字手续。对于需要送修和销毁的介质，须确保存储内容的清除和不可恢复。

第十二条　系统工作人员须妥善保管信息载体，不得出借、出售或转予第三方，不得随意在他人电脑或者无加密环境下使用存储重要信息的载体。

第十三条　需携带保密载体外出的，必须经单位领导批准，必要时实行双人外出制。

第十四条　需通过电子载体传输信息的，应当做好存储介质在物理传输过程中的安全控制，选择可靠的传递方式和防盗控制措施。重要信息的存取需要授权和记录。

第十五条　加强对服务器、网络设备、用户端设备的登记和规范化管理，确保按操作规程实现硬件设备的使用与维护。禁止外来硬件设备的擅自接入，禁止私自拆卸、添加或销毁硬件设备，禁止私自送修硬件设备。市信用平台相关硬件设备必须经过审核登记才能带离机房或办公地点。

第十六条　硬件设备每月至少检查一次，确保其安全稳定运行。建立关键设备使用情况登记表，及时记录设备使用中出现的各种症状，上报异常情况，做好故障预防。

第十七条　市信用平台各终端计算机和服务器必须安装使用正版防病毒软件，并定期更新升级，定期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。不得安装其他无关软件。

第五章　系统账号管理

第十八条　市信用平台数据及其产生的各类信用记录、信用报告、统计分析报告等信用成果的开放权限，由市信用办统一设置、统一批准，并按相关要求与使用单位签订协议，任何单位或个人未经批准不得使用或向第三方提供系统数据和成果。

第十九条　账号申请实行“实名制”管理，每人仅能申请一个账号。系统工作人员之间不得随意借用、串用账号，因账号操作造成信息泄露、数据或系统功能等方面的改变，后果均由拥有该账号的人员及单位负责。

第二十条　系统工作人员在首次登陆市信用平台后，应立即修改初始密码，并做到定期更换新密码。

第二十一条　系统工作人员岗位调动或离职前,其所在单位应及时更换新密码。

第二十二条　系统工作人员若发现账号密码泄露,应立即口头报告市信用办停用账号，并在 24 小时内提交书面报告，说明详细情况，避免损失扩大。

第六章　应急管理

第二十三条　建立健全应急反应机制，针对发生数据窃取、网络攻击、服务器入侵、数据库崩溃等情形，制定相应的应急预案，定期开展应急培训和演练。市信用平台每年至少进行一次灾难恢复演练。

第二十四条　市信用平台发生信息安全事件后，系统工作人员应立即报告本单位主管领导和市信用办，注意保护事件现场，采取必要的控制和灾难恢复措施，避免影响范围的扩大。事后应及时调查、分析事件原因，报告市信息安全主管部门。如发生重大信息安全事件，还应向公安机关报案。

第七章　档案管理

第二十五条　市信用平台用户单位所掌握的公共信用信息以及依托公共信用信息产生的各类查询报告、统计分析报告、其他相关信用成果，以及相关的公文材料等应严格按照规定进行保管，实行档案登记管理制度。

第二十六条　各种业务档案及公文材料等应按组卷要求，由立卷人整理，按有关规定装订并移送档案室统一保管。

第二十七条　档案管理人员和借阅人员必须严格遵守国家保密法及单位各项保密制度，认真做好保密工作。任何人不许将档案内容泄露给无关人员。

第二十八条　档案管理人员应严格执行档案查阅、借阅制度；履行登记手续，认真审查审批权限是否符合规定的要求。

第二十九条　档案材料应尽量现场查阅，原则上不允许借出查阅。如因工作需要，确需外借档案材料的，应当获得借出单位分管领导的批准。经批准后，由档案管理人员履行登记手续，方可借出。借出的档案材料务必定期归还。借出使用期间，不许转借他人，不许带入公共场所。

第三十条　如需销毁档案，须经专人清点、核对、登记、造册，由本单位专人销毁。对销毁的时间、地点、方式及销毁过程中存在的问题进行记录，与销毁清册一并存档。

第三十一条　档案要做到安全保管，定期检查，做到防盗、防火、防潮、防尘、防失密，保持经常通风。

第八章　附则

第三十二条　本办法由市信用办负责解释。

第三十三条　本办法自印发之日起实施。

附件 2：

黑河市信用信息共享平台信息安全组织及职责管理规定

第一章　总则

第一条　为了加强的统一管理，确定信息安全管理的组织机构和职责，特制定本规定。

第二条　本规定适用于综合管理和相关岗位的安全职责。

第二章　相关岗位信息安全职责

第三条　安全管理员不能兼任网络管理员、系统管理员、数据管理员,信息安全组织中设置信息安全岗位,并明确各岗位安全职责。

第四条　信息安全工作主管的岗位职责如下：

（1）组织、协调落实各项信息安全工作；

（2）组织评审信息安全总体策略、规划方案、管理制度和技术规范；

（3）组织监督、检查信息安全工作的落实情况。

第五条　安全管理员的职责如下：

（1）定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况；

（2）组织信息系统的安全风险评估工作，形成安全现状评

估报告，并向安全主管报告信息安全整体情况；

（3）负责制定总体网络访问控制策略和规则，并对其进行监控和审计工作，定期发布策略执行情况；

（4）负责制定全员的安全培训计划，组织开展安全培训工作；

（5）负责沟通、协调和组织处理信息安全事件，确保信息安全事件能够及时处置和响应。

第六条　网络管理员的安全职责如下：

（1）负责网络及安全设备的配置、部署、运行维护和日常管理工作；

（2）负责编制网络及安全设备的安全配置标准；

（3）能够及时发现、处理网络及安全设备的故障和相关安全事件，并能及时上报，减少信息安全事件的扩大和影响。

第七条　数据管理员的安全职责如下：

（1）负责数据的备份、恢复、测试及安全存储；

（2）负责数据存储、备份以及存储备份设备的日常安全运行管理工作；

（3）能够及时发现、处理数据存储和备份的相关安全事件，并能根据流程及时上报，减少信息安全事件的扩大和影响。

第八条　系统管理员的安全职责如下：

（1）负责服务器和终端的日常安全管理工作，确保操作系统的漏洞最小化，保障主机设备安全稳定运行；

（2）负责编制操作系统的安全配置标准；

（3）能够及时发现、处理主机和操作系统相关安全事件，并能根据流程及时上报，减少信息安全事件的扩大和影响。

第九条　应用管理员的安全职责如下：

（1）负责支持和协助所管辖应用系统中涉及信息安全的相关标准、规范与管理制度建设；

（2）负责对所管辖业务应用系统进行安全配置，负责应用系统设计、实施和运维的信息安全管理工作；

（3）责对所管辖业务应用系统的用户权限分配和管理，对登录用户进行监测和分析；

（4）负责实施系统软件版本管理，应用软件备份和恢复管理；

（5）负责监督和管理第三方应用系统开发时的安全管理工作；

（6）能够及时发现、处理应用系统相关的安全事件，并能根据流程及时上报，减少信息安全事件的扩大和影响。

第十条　安全审计员不能兼任网络管理员、系统管理员、数据管理员和安全管理员，安全审计员的职责如下：

（1）定期审计信息安全制度执行情况，收集和分析信息系统日志和审计记录，及时报告可能存在的问题；

（2）对安全、网络、系统、应用、数据库管理员的操作行为进行监督，对安全职责落实情况进行检查。

第十一条机房管理员的主要安全职责包括：

（1）负责机房内的配电设备、UPS、空调机等基础设施的维护与管理 ，并负责对机房设备的相关介质、文档资料等随机物品进行归档管理。

（2）负责机房相关设备的日常维护管理与操作 ；

（3）负责非技术性的、常规的安全工作，如机房的保卫，验证出入手续和规章制度的落实等。

第十二条资产管理员的安全职责如下：

负责物理资产的采购、登记、分发、回收、废弃等安全管理工作。

第十三条　其他员工安全职责如下：

（1）落实执行各类信息安全管理要求，加强信息安全知识的学习，提高信息安全意识；

（2）确保使用各类信息资产的保密性、可用性和完整性。

第三章　授权和审批

第十四条　各部门需要明确各自的岗位和职责，部门内实行逐级审批制度。

第十五条　审批流程要按照如下几个流程进行：提出申请、相关负责人审批、审批通过、　登记记录、备案归档。

第十六条　针对系统的变更或重要操作，需要向信息提出申请，要明确变更内容或操作过程，以及分析可能的影响，待审批通过后，方可进行变更或操作，具体参考《信息系统变更管理规

定》。

第十七条　出入机房等，需要填写机房出入登记表，并经允许后方可出入，具体参考《机房环境安全管理规定》。

第十八条　机房新增设备或系统，要在信息报备并经许可后方可实施。

第十九条　应对审批过程进行记录并保存审批的文档。

第四章　沟通和协作

第二十条　为更高效的处理信息安全问题，应加强内部部门、人员之间的合作与沟通，共同参与安全规划和评审，对信息安全重要问题的决策提供咨询和建议。

第二十一条　应加强与兄弟单位、公安机关的合作与沟通。

第二十二条　应能够与网络链路提供机构、信息系统运维机构、信息系统的硬件设备、软件设备提供商保持合作，确保在出现各类安全问题时能够沟通顺畅。

附件 3：

黑河市信用信息共享平台内部人员安全管理规定

第一章　总则

第一条　为进一步加强内部工作人员的安全管理工作，明确内部人员在被录用前、工作期间以及调岗和离职各个过程中的安全管理要求，特制定本规定。

第二条　本规定中的内部人员（以下简称“人员”）是指涉及信息系统使用、运行维护、建设和管理的内部工作人员。

第二章　组织和职责

第三条　安全主管负责审定信息安全相关部门和岗位的安全职责，确定信息安全关键岗位人员的能力，监督、考核信息安全关键岗位人员工作绩效，确定信息安全违规行为的处罚措施。

第四条　安全管理员负责制定信息安全相关部门和岗位的安全职责，组织落实安全主管对于内部人员的各类安全要求。

第五条　办公室负责人员在录用、培训、考核、调岗和离职过程中的管理工作。

第三章　人员录用

第六条　录用部门应明确被录用人员的专业资格与技术技

能要求，并依据技能要求对其进行考核。

第七条　办公室负责审核被录用员工的背景、身份、履历的真实性，确保符合相关法律法规、业务要求和道德规范要求。

第八条　信息安全关键岗位人员应优先从内部人员中选拔，并签署保密协议。

第四章　工作期间安全管理

第九条　信息安全工作组应制定安全教育和培训计划，对员工信息安全基础知识、岗位操作规程、安全技术等进行培训。

第十条　新员工正式上岗前后应接受一次信息安全意识培训，明确所要遵守的信息安全管理制度和规范。

第十一条　针对信息系统的维护人员和管理人员应定期开展安全技术培训，明确如何安全使用各业务系统、主机操作系统以及普通计算机周边硬件设备等。

第十二条　应定期开展由供应商或厂家提供的专业安全技术培训，帮助相关安全管理人员和技术人员了解掌握正确、安全地安装、配置、维护系统。

第十三条　各部门应根据员工的岗位职责和岗位要求，严格控制和管理人员的信息资源访问权限。

第十四条　各部门人员在发生岗位变更后，应根据岗位要求进行信息、信息资产使用和访问权限的变更，合理控制人员对于信息资源的访问。

第十五条　各部门把信息安全作为人员绩效考核的一部分，

包括：

（1）把信息安全意识列入考核范围，加强全员对于信息安全整体的防范能力；

（2）对涉及信息安全管理、检查和执行的岗位人员，应定期进行安全技能的考核，包括安全管理知识的掌握程度、所管理业务系统中安全产品的操作技能、所管理业务系统中使用的操作系统和应用软件的安全使用等；

（3）将发生的安全事故、安全检查结果和安全审计结果纳入考核内容。

第十六条　对于违反信息安全管理制度的人员，依照违规程度确定具体的惩戒措施，严重违法者应移交至司法部门。

第五章　人员调岗、离岗

第十七条　人员在调岗和离岗过程中，应依照保密协议进行审定，确保不会因此对的业务造成安全风险。

第十八条　系统管理员应及时终止调岗、离岗人员的访问权限，对调岗人员的访问权限应根据新岗位的访问权限重新设置。

第十九条　人员离岗时应经部门内主管领导确认信息处理设备上的信息已经及时进行清除，并确保信息资产的及时归还，保证其完整性和安全性。

黑河市信用信息共享平台
外部人员安全管理规定

第一章　总则

第一条　为加强对外部人员在的信息安全管理，防范外部人员带来的信息安全风险，规范外部人员在信息系统中的各项与信息系统相关的活动所要遵守的行为准则，特制定本规定。

第二条　本规定适用于的外部人员安全管理工作。

第二章　定义

第三条　本规定中外部人员包括软件开发商、产品供应商、系统集成商、设备维护商、服务提供商、业务合作伙伴、临时雇工、实习生等外来人员，外部人员分为临时外部人员和非临时外部人员。

（1）临时外部人员指因业务洽谈、技术交流、提供短期和不频繁的技术支持服务而临时来访的外部人员；

（2）非临时外部人员指因从事合作开发、参与项目工程、提供技术支持或顾问服务，必须在相关单位办公的外部人员。

第四条　接待人是指受访部门派出的、负责接待外部人员的接口人。

第三章　外部人员风险识别

第五条　各部门在与外部人员进行接触过程中，应防范外部人员对于可能带来的各类信息安全风险，这些风险包括但不限于

如下内容：

（1）外部人员的物理访问带来的设备、资料盗窃；

（2）外部人员的误操作导致各种软硬件故障；

（3）外部人员对资料、信息管理不当导致敏感信息泄露；

（4）外部人员对计算机系统的滥用和越权访问；

（5）外部人员给计算机系统、软件留下后门；

（6）外部人员对计算机系统的恶意攻击。

第四章　外部人员管理要求

第六条　临时外部人员进入时，接待人必须全程陪同，告知有关安全管理规定,未经允许不得使用的计算机和电子网络设备。

第七条　非临时外部人员必须签署安全保密协议后才能进场工作。

第八条　业务洽谈和技术交流应当会议室进行，招标、谈判等正式洽谈和重大项目的会谈应当在专门的会议室进行。

第九条　外部人员进入机房等重要区域时，应遵从《机房环境安全管理规定》等规定。

第十条　未经相关领导许可，外部人员不得在办公区域、设备间、机房等关键区域摄影、拍照。

第十一条　在未经相关部门主管领导的审核审批的情况下，禁止外部人员了解和查阅的敏感、重要信息、文档等。

第十二条　外部人员如因业务需要查阅敏感资料或访问网络和信息系统资源，必须经过安全管理员批准并详细登记。

第十三条　未经允许，禁止外部人员远程访问网络。如确因工作需要（例如维护、故障处理）需要远程访问，必须经安全管理员批准并详细登记。

第十四条　外部人员在机房内的所有操作，都必需说明该操作可能引起的安全风险，并由接待人认可后才能操作。接待人必须对外部人员的操作进行全程监控，记录外部人员的操作内容并存档备案。

第十五条　外部人员对机房附属设备（如空调、UPS 等）的维护和保养，事先要由接待人员上报相关部门主管领导批准后选择合适的时间进行，确保操作不影响系统的正常运行。

第十六条　未经批准，禁止外部人员携带移动存储介质进入机房。

第十七条　外部人员如因工作需要使用移动存储介质，必须在接待人的监控下使用，由此而产生的安全风险由接待人承担。

附件 4：

黑河市信用信息共享平台安全审核和安全检查制度

一、工作目标

发现问题，排除隐患，消除薄弱环节，通过对信息系统安全现状的全面检查，分析了解当前网络和信息系统的安全漏洞、隐患和主要安全问题，有针对性地提出整改措施，完善信息系统安全防护体系。

二、检查范围

安全检查分为日常安全检查和全面安全检查两种。日常安全检查周期为每月一次，全面安全检查为每年一次。

日常安全检查内容包括系统日常运行、系统漏洞、数据备份、备份恢复等，由信息安全科负责监督检查过程，检查报告、结果通报情况等工作。

全面安全检查内容包括现有安全技术措施的有效性、安全配置与安全策略的一致性、安全管理制度的执行情况等，由网络与信息安全领导小组办公室负责监督检查过程，落实解决措施，检查结果通报等工作。

三、检查方法

检查方法有人员访谈、资料检查、工具测试三种。安全检查

的实施阶段划分如下：

（一）被检查对象配合实施人员如实回答问题，提供相关文档，配合测试，确认检查结果。

（二）整理检查结果，汇总相关数据和文档，按相关标准将检查结果进行分类，列出成绩突出的和存在严重问题的被检查对象。

（三）通过检查暴露出来的问题要逐一进行分析，提出详细的整改要求。

（四）以通告的方式将检查结果和详细整改方案告知被检查对象。

（五）对安全整改措施的落实情况进行监督检查，并记录整改后情况和结果。