淮安市公共信用信息中心

淮公信〔2016〕8号

淮安市信用信息安全管理暂行办法

第一章　总则

第一条 为保障淮安市公共信用信息系统（以下简称市信用系统）信息安全，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》及有关法律法规，结合工作实际，制定本办法。

第二条 本办法适用于淮安市信息中心（市公共信用信息中心，以下简称市信用中心）各处室及所有职工。

第三条 本办法所称信息安全管理，是指在市信用系统及相关项目立项、建设、运行、维护及废止等过程中保障计算机信息及其相关系统、环境、网络和操作安全的一系列管理活动。

第二章　人员管理

第四条 信息安全管理工作由信用信息中心、网络管理处和综合处及相关职能处室共同实施，每年定期或不定期进行信息安全联合检查。检查中一旦发现问题或者隐患，相关人员及处室要立即整改，加强防范措施。

第五条 市信用中心员工应维护公共信用信息及相关资料档案安全、保守单位秘密，自觉遵守有关法律法规和内部制度，并接受保密教育和监督。

第六条 市信用中心员工（包括政务大厅窗口人员）的选拔，须严格遵守相关标准及要求。聘用编外或实习生需签订保密合同。严禁临时人员（包括实习生）从事公共信用信息的查询、统计分析、监测预警等工作。

第七条 市信用中心员工上岗前，必须参加公共信用信息安全培训，并与单位签订保密协议书，承担保密责任、履行保密义务。

第八条 市信用中心员工应当严格按照内部制度、岗位职责和操作权限操作系统。不得将操作账号转予他人使用，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 员工办理轮岗、离职、退休手续时，应将所接触或掌握的保密信息，向市信用中心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。

第三章　信息载体管理

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、U 盘、磁盘、磁带、缩微胶片及纸质资料等载体。

第十一条 信息载体须由信息安全保障专员管理，载体的发放、更换和销毁等均须履行登记签字手续。

第十二条 市信用中心员工需妥善保管信息载体，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 因工作需要须携带保密载体外出的，必须经市信用中心领导批准。必要时实行双人外出制。携带重要信息载体外出应采取必要的保密措施。

第十四条 因工作需要须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。

第四章　系统及账号管理

第十五条 信息安全保障专员应在开通账号时，设置初始密码。用户应在取得初始密码后立即更改密码。用户密码的设置应尽量复杂化，不易被他人推测，密码长度一般不少于10位，并做到定期更换新密码，密码遗忘时可申请密码初始化修复。同时，

系统自动检测账号，判定为不安全时，暂时封锁该账号。

第十六条 账号申请实行“实名制”管理，工作人员之间不得随意借用、串用账号，因某工作人员账号的操作而信息泄露、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负责。

第十七条 如工作人员因岗位调动、离职或退休等原因而不允许继续使用相关系统时，信息安全保障专员应在人员调动、离职或退休前注销用户账号；不论原工作人员是否知晓或同意，均禁止将其原账号转交其他人员继续使用。

第十八条 若发现账号密码泄露，工作人员须立即口头报告信息安全保障专员，并及时采取停用账号措施。在报告后的24小时内向该信息安全保障专员和中心领导提交书面报告，说明详细情况。信息安全保障专员应在接到口头报告后第一时间反应修复，避免损失扩大化。

第十九条 工作人员离开操作用机时，应按程序退出系统，回到操作系统初始状态，防止业务数据被复制、修改、删除以及误操作。

第五章 计算机和机房管理

第二十条 业务操作计算机系统或单机，应设置用户登陆密码并定期更换。不得直接或间接与互联网、公共信息网相联接，不得在未采取数据保护和网络安全保密监控管理技术措施的计算机网络内输入、保存和传递保密资料的信息。非加密计算机信息

系统不得采集、存储、处理、传输保密信息。

第二十一条 凡需要在“诚信淮安”网站上进行信息发布的，应当认真执行信息保密审核制度，经过市信用中心领导批准后，统一信息发布专员对外发布。严禁私自通过网络传递市信用中心产生或掌握的公共信用信息、内部资料以及重要公文等内容。

第二十二条 计算机信息系统应定期维护。如需更换或维修的，应由信息安全保障专员协同实施。所更换的设备或配件，在未采取技术处理时，不得挪为他用。

第二十三条 机房场所应当安全保密，建立和健全机房管理制度，采取必要的技术措施保障信息安全。

第二十四条 对需报废的计算机设备及其配件，应当登记造册，经中心领导批准后，方可销毁。具体操作参照《事业单位固定资产管理办法》执行。

第二十五条 任何部门和个人在发现信用系统信息存在隐患或已发生问题时，应及时采取补救措施，并立即上报信息安全保障专员和中心领导。

第六章 档案管理

第二十六条 市信用中心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，以及市信用中心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。

第二十七条 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市信息中心档案室统 一保管。

第二十八条 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。

第二十九条 档案管理人员须严格执行档案查阅借阅制度；履行借阅登记手续，认真审查审批权限是否符合规定的要求。

第三十条 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，应当获得中心领导的批准。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。

第三十一条 涉及市信用中心重要业务资料和公文材料的，必须经中心领导批准后再作借阅，严防泄密。

第三十二条 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。

第三十三条 非档案管理人员，未经批准不得进入档案室。

第三十四条 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。

第七章 外包管理

第三十五条 外包服务是指由市信用中心之外的企事业单位

为市信用中心、市信用平台系统以及网络建设等方面提供全面或部分的技术支持、咨询等服务。外包服务应签订正式的外包服务协议，并明确外包服务提供商的保密义务。

第三十六条 外包服务提供商不得查看、复制涉密信息或将涉密介质带离市信用中心。需长期合作的，应与外包服务提供商签订保密协议。

第八章 应急管理

第三十七条 重大信息安全事件发生后，各相关人员应注意保护事件现场，采取必要的控制措施，调查事件原因，并及时报告本单位主管领导。

第三十八条 建立健全应急反应机制，定期开展应急演练和培训。在条件许可的情况下，重要信息系统至少每年进行一次灾难恢复演练，包括异地备份站点切换演练和本地系统灾难恢复演练。

第三十九条 制定并不断完善网络系统、市信用平台和数据中心机房环境等相关应急预案。在推进业务系统应用同时，应设计应急备份策略，同步实施备份方案。

第九章 安全监测和检查

第四十条 整合和利用现有网络管理系统、计算机资源监控系统、专用安全监控系统以及相关设备与系统的运行日志等监控资源，加强对网络、重要计算机系统和机房环境等设施的安全运行

监测。

第四十一条 建立运行监测月报制度，报送中心信息安全工作领导小组。

第四十二条　至少每半年在本单位组织 1 次信息安全专项检查，安全检查方式可以是自查、互查或上级检查多种方式。

第四十三条 开展安全检查应以安全管理制度为依据制定详细的检查方案和计划，确保检查工作的可操作性和规范性。安全检查完成后应及时形成检查报告，经中心主管领导批准后将检查整改报告尽快送达被检查部门。要求限期整改的，需要对相关整改情况进行后续跟踪。

第十章　附 则

第四十四条 本办法由市公共信息中心负责解释。

第四十五条 本办法自 2016 年 9 月 1 日起施行。

淮安市公共信用信息中心

2016 年 8 月 9 日