淮安市公共信用信息中心

淮公信〔2016〕1号

淮安市公共信用信息工作人员管理规范

第一章　总则

第一条　本规范规定了淮安市公共信用信息中心（简称：信用中心）机构及工作人员主要职责。

第二条　本规范适用于信用中心内部管理参考用。

第二章　机构与职责

第三条　信用中心承担全市公共信用信息归集、数据管理、共享交换、发布应用，为行政管理提供信用信息服务，为社会提供公共信息查询服务的机构。

第四条　机构职责

（一）承担信用信息平台的建设和运行，负责数据库的开发和日常维护；根据公共信用业务逐步扩大的需求，对信用信息平台进行系统升级和改造；负责系统运行的

安全管理。

（二）负责依法征集各有关部门、各县区以及经授权或者委托承担行政管理职能的组织的履行职责过程中生成的信用信息的征集、加工、交换和服务工作；负责全市公共信用信息中心的业务指导和技术支持。

（三）承担为各有关部门和各县区提供信用信息服务，为社会提供公益性信用信息查询服务；承担跨地区的信用信息交换和共享工作；负责受理信用信息异议、信用投诉等工作。

（四）为联动监管工作提供信息服务和技术服务；负责市信用信息联动监管、绩效统计，并报信用办进行相应业绩考核工作。

（五）协助信用办做好公共信用体系建设工作；承担交办的企业、个人信用信息体系建设的政策、法规、规划等课题研究工作。

（六）承担江苏省、市委、市政府、市社会信用体系建设领导小组及其办公室交办的其他事项。

第三章　系统管理员主要职责

系统管理员主要职责包括网络管理、平台管理和应用系统管理三部分。

第五条　网络管理

（一）负责系统网络基础设施（线路、网络设备、网络软件、

网络配置等）的日常管理和维护，确保网络系统安全、稳定、高效地运行。

（二）负责网络运行状态的监控、管理及运行维护。

（三）每日记录网络运维和管理状态，发现异常及时处理并报相关领导。

（四）每月向相关领导报送当月网络运行和管理情况及各种网络事件。

（五）负责协助安全管理员分析网络隐患，制定安全策略。

（六）负责协助领导制定、补充、完善系统管理制度。

（七）负责管理网络系统建设、运行的相关文档。

（八）负责网络系统的规划工作。

第六条　应用管理

（一）负责公共信用信息平台中各应用系统的日常管理和维护，确保应用系统安全、稳定、高效地运行。

（二）负责各应用系统运行状态的监控、管理及运行维护。

（三）负责每日记录应用系统的运维和管理状态，发现异常及时处理并报相关领导。

（四）负责每月向相关领导报送当月应用系统运维和管理情况。

（五）负责定期对系统用户权限进行审查，及时掌握变更情况，按照最小授权原则对系统用户进行权限变更处理，更新用户权限列表并及时上报相关部门。

（六）负责定期进行系统数据备份，并在安全事件发生时及

时处理，尽快恢复。

（七）负责应用系统的日志分析，预防系统安全事件的发生。

（八）负责应用系统结构和性能的优化。

（九）负责协同安全管理员定期对应用系统进行软件升级和补丁安装。

（十）负责协助领导制定、补充、完善系统管理制度。

（十一）负责管理应用系统建设、运行的相关文档。

（十二）负责应用系统的规划。

第七条　　平台管理

（一）负责主机系统及存储系统硬件和软件的日常管理和维护，确保系统服务器安全、稳定、高效地运行。

（二）负责各服务器运行状态的监控、管理及运行维护。

（三）负责对系统服务器进行安全策略配置。

（四）负责主机操作系统的日常维护和升级工作，负责服务器操作系统的状态监控，及时掌握各主要服务器系统的使用情况，及时发现非法程序、病毒、蠕虫、木马程序入侵系统。

（五）负责协同安全管理员定期对系统内服务器进行病毒扫描、漏洞扫描并进行补丁安装和软件升级。

（六）负责定期检查系统内平台设备和存储设备的运行状态，并做好日志的记录。

（七）负责协助安全管理员制定安全策略，确保主机平台的安全、稳定、高效地运行。

（八）负责协助领导制定、补充、完善系统管理制度。

（九）负责管理平台系统建设、运行的相关文档。

（十）负责主机系统及存储系统的规划

第四章　　安全管理人员主要职责

安全管理主要职责包括安全管理、安全审计管理二部分。

第八条　　安全管理员

（一）负责系统的安全管理工作，负责系统安全策略的规划和制定。

（二）负责系统安全状态的监控、管理。

（三）负责系统安全设备和软件的管理、使用和维护。

（四）负责系统安全设备和软件的状态监控，每月对安全产品的有效性进行检查，及时掌握安全设备和软件的运行情况。

（五）负责系统安全设备和软件的升级更新、故障处理。

（六）负责根据系统变化情况进行风险评估，及时调整系统保护策略。

（七）接受来自系统用户的安全事件报告，并及时处理。

（八）负责系统安全产品的日志分析，定期对重要安全产品的日志进行分析整理，及时找到不正常事件或隐患。

（九）负责定期向相关领导报送系统安全管理情况和安全事件处理情况。

（十）负责协助领导制定、补充、完善安全管理制度。

（十一）负责管理安全的相关文档。

（十二）安全管理员。

第九条　　安全审计员

（一）负责对系统管理员、安全管理员的操作行为进行审计、跟踪分析和监督检查并形成审计记录。

（二）负责对服务器、重要涉密终端和安全设备的操作行为进行审计并形成审计记录。

（三）负责对服务器的操作行为进行审计并形成审计记录。

（四）负责对系统审计功能的启动和关闭进行审计。

（五）负责对系统所生成的审计记录进行审计。

（六）负责对系统内用户的增删、权限更改等操作进行审计并形成审计记录。

（七）负责对系统安全策略执行情况进行审计并形成审计记录。

（八）负责对系统内其他与安全有关的事件或行为进行审计并形成审计记录。

（九）当审计发现问题时及时向安全管理单位汇报。

（十）负责每月根据审计记录，形成文档化的安全审计报告。

（十一）负责协助领导制定、补充、完善能确保审计策略正确实施的管理制度。

（十二）负责确定安全审计范围、制定安全审计策略并将其文档化。

第五章　操作终端人员主要职责

第十条　使用人员

（一）公共信用信息系统中所有的计算机必须安装指定的杀毒软件产品。

（二）系统终端用户应每周进行至少一次病毒与恶意代码查杀，及时清除被隔离和未被删除的病毒，不得自行关闭杀毒软件的实时监控功能，如果出现自动关闭的情况，应立即通知相关部门解决。

（三）终端用户可自动升级计算机病毒库，如发现病毒库版本没有自动升级应及时通知系统管理员。

（四）终端计算机必须安装系统的安全补丁，终端用户必须接受 WSUS 升级服务，以便自动获取补丁。

（五）计算机硬盘应尽可能分区，并将文档、数据集中存放在系统分区以外的分区中。

（六）用户定期备份本机文件，一旦病毒破坏了数据，可利用存储档案恢复相关文件。

（七）严禁在计算机上随意安装软件。如需安装与工作有关的软件，须经相关安全管理部门审批后才能安装使用。

（八）使用移动存储介质拷贝文件时，须进行计算机病毒的查杀。

（九）凡因任意安装软件、使用非工作存储介质导致操作系统崩溃或传播病毒的用户，一经查实，将依法严肃处理。

（十）如发现计算机出现如下症状时，应及时通知系统管理员，并保护现场（暂时停止工作以防止病毒的扩散）：计算机瘫痪，程序和数据被严重破坏，或者网络出现严重故障等。屏幕显示异常、屏幕显示出不是由正常程序产生的画面或字符串、屏幕显示混乱。程序装入时间增长， 文件运行速度明显下降。用户没有访问的设备出现工作信号。磁盘出现莫名其妙的文件和坏块，卷标发生变化。系统自行引导。丢失数据或程序，文件字节数发生变化。内存空间、磁盘空间异常减小。异常死机。磁盘访问时间比平时显著增加。系统引导时间增长。

第六章　附则

第十一条　本规范自 2016 年 1 月 1 日起实施。

第十二条　本规范由淮安市公共信用信息中心负责解释。

淮安市公共信用信息中心

2016 年 1 月 1 日