天津市红桥区信用信息共享平台
人员管理制度
（试行）

第一章　安全管理人员及职责

第一条 系统管理员职责

系统管理员分为网络管理员、主机管理员和数据库管理员。

一、网络管理员职责:

网络管理员负责信用平台承载网络“天津市红桥区电子政务专网”的网络安全管理和日常运行维护的网络安全管理和日常运行维护。

（一）负责信用平台承载网络的规划与部署，确保信用平台网络的畅通，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）每月月底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。

二、主机管理员职责:

（一）负责信用平台应用服务器、数据库服务器及前置机操作系统的配置与管理，保持主机设备处于良好的运行状态，负责主机设备的正常启动与关闭。

（二）负责主机操作系统应用软件的安装，从系统层面实现对用户与资源的访问控制。

（三）每天定时查看主机设备运行日志，了解承载主机运行状况，在主机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）每月月底对主机设备硬件进行检查与维护。

（五）协助安全管理员制定主机操作系统的安全配置规则，并落实执行。

（六）为安全审计员提供完整、准确的主机系统运行活

动的日志记录。

（七）负责编制主机设备的维修、报损、报废计划。

（八）负责对主机操作系统配置文件进行备份，及时修补主机操作系统的漏洞。

（九）严格执行各项保密制度，做到授权信息绝不外泄。

三、数据库管理员职责

（一）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。

（二）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，每周对数据库系统升级，管理数据库的存储、备份、安全和日志等工作。

（三）具体负责数据库维护管理任务，如创建数据库实例、管理补丁、数据库导入/导出、数据库性能调试、用户管理等。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。

（四）参与数据库环境的灾备计划的制定、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。

（五）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。

（六）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。每周检查数据库资源联通性、自动备份情况、口令定期修改情况以及对主机系统 CPU 和内存的占用情况等，并填写《数据库检查列表》。

（七）按规定授权原则确定不同用户的数据访问权限，并由专人负责编制授权表。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。

（八）不得随意在数据库中查询、拷贝信用信息数据。

（九）每月月底对数据库日志进行分类、归纳，总结当月安全及生产运行情况，编写数据库服务运行支撑月报，交领导审阅并归档。

第二条 安全管理员职责

一、协助制定系统建设和发展安全规划，组织并实施年度安全计划。负责系统安全的管理，协调各部门实施系统安

全有关管理措施。

二、每天监控安全设备和安全软件运行状态，及时了解安全设备和软件运行情况，每月审查权限列表。

三、负责安全设备或软件部件升级更新、故障处理。

四、负责安全产品日志分析，随时监督网络情况，并对重要安全产品日志进行分析整理，形成《安全分析记录单》；及时发现黑客入侵、病毒侵害等安全隐患并妥善处理。

五、负责服务器的防病毒和防篡改工作，对服务器进行定期查毒、杀毒，及时下载并安装系统漏洞补丁，采取各种有效措施防止黑客攻击和破坏。

六、对系统运行环境进行安全维护，做好机房防雷、防火、防水和防潮、防盗窃和防破坏和防虫害措施。

七、负责制定安全检查表格，每月月底对系统日常运行、系统漏洞和数据备份等情况进行安全检查，每季度对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进行全面检查，根据检查情况填写《系统安全漏洞检测记录表》、《网络系统安全性能检测表》、《应用系统安全性能检测表》和《服务器安全性能检测表》；检查后汇总安全检查数据，形成《安全检查报告》。

八、负责配合上级机构及监管部门执行网络安全检查。

九、受理信息系统安全事件报告。

十、每月向领导小组办公室报送安全管理情况和异常事

件统计信息。

十一、严格执行各项保密制度，做到授权信息绝不外泄。

第三条 安全审计员职责

一、定期（每周）对信用平台各类操作人员的操作行为进行审计和监督，根据审计和监督情况填写《安全审计记录表》。

二、定期（每周）对系统安全策略及各项安全规章制度的执行情况进行审计和监督，根据审计和监督情况填写《安全审计记录表》。

三、定期（每月）对信用平台各用户名和口令的管理与变更记录进行审计和监督，根据审计和监督情况填写《安全审计记录表》。

四、定期（每月）对系统管理员、安全管理员等其他管理人员的工作和相关文档进行符合性检查，根据检查情况填写《符合性检查记录表》。

五、负责对所有审计事项的审计结果进行记录，及时发现安全隐患，提出处理意见和建议，形成审计报告，并及时报领导小组办公室审核。

六、对审计的安全事件进行及时处理，记录处理结果。

七、定期（每周）备份安全审计日志，并负责做好审计资料的收集、整理、建档工作。

八、严格执行各项保密制度，做到授权信息绝不外泄。

第四条 数据管理员职责

一、对自然人数据及其他信用数据的登记、保管。

二、记录好接收数据的时间、文件名称、大小、数据内容、数据入库时间等。

三、负责规划数据的存放位置，并做好台账登记。

三、负责各信源单位自然人数据及其他信用数据的整理、上传和下载。

四、负责自然人数据及其他信用数据存储介质及相关秘钥的的存放和管理。

五、负责对数据存储介质进行保管，对存储介质的借入借出进行管理。

六、负责存储介质定期检查，考虑存储介质的安全保存期限，及时更新复制。损坏、废弃或过时的存储介质应及时销毁。

七、负责对外提供、发布数据，并提供数据解释。

第五条 应用管理员职责

一、负责信用平台的安装、调试，做好系统上线、数据移植工作。

二、负责按照权限分配表在信用平台中设置用户的权限，

对应用系统的用户、口令的安全性进行管理，对应用系统的登录用户进行监测和分析。

三、负责实施应用系统版本管理、应用系统备份和恢复管理。

四、负责提出数据的备份要求，制定数据备份策略，督促数据库管理员按照备份方案按时完成，并恢复所需数据。

五、负责解决并记录应用系统中的问题，督促开发人员提供补丁来修补已发现的漏洞。

六、协助安全管理员制定应用系统安全配置规则，并落实执行。

七、为安全审计员提供完整、准确的应用系统运行活动的日志记录。

八、负责应用系统有关资料整理并及时归档，确保系统技术资料保存完好。

九、根据实际运行情况和业务部门的要求对新增功能进行调试和培训，并编制相应的操作手册。

十、严格执行各项保密制度，做到授权信息绝不外泄。

第二章　人员安全管理规定

第六条 内部工作人员管理

一、选拔任用信用平台工作人员，要依据信息安全相关

标准要求，进行严格审查，包括录用人员的身份、背景、专业资格和资质等进行审查和核实。

二、应从内部人员中选拔从事关键岗位的人员，并签署岗位安全协议，不应录用有过刑事犯罪纪录的人员，不符合要求的人员应及时调离岗位。

三、应将所有工作人员岗位职责文档化，并要求其签字确认。

四、信用平台工作人员工作活动场所和工作信息接触范围应当被限制在完成本职工作所需的最小范围内。

五、领导小组办公室应定期对信用平台工作人员进行信息安全教育、培训和考核。

六、信用平台管理人员办理离岗离职手续时，须签署离岗保密协议书，承诺保密义务后方可离岗。即时取消其一切授权，注销用户账号，收回机构提供的各种身份证件、钥匙、软硬件设备等。

七、为进一步明确工作责任，提高工作效能，特针对关键事务岗位制定 AB 角工作制度:

1、AB 角工作制度是指 A 角不在岗的情况下，由 B 角负责顶岗的工作制度。各岗位人员应对本岗位承担的各项工作进行合理分工及安排，认真落实 AB 角制度，避免出现无人顶岗现象。

2、各岗位人员在安排工作时，原则上保证 AB 角有一人

在岗。互为 AB 角的人员，原则上不能同期休假，不能同时出差。

3、B 岗责任人在顶岗期间，应做好本职工作，并负有 A 岗责任人的职责，对 A 岗的工作认真负责。

4、全体人员应加强学习，AB 角之间要不断地进行相互沟通，A 角暂离岗位时，要切实做好交接工作，确保 B 角能够衔接到位。

第七条 外部工作人员管理

一、须向外部人员明确信用平台的相关规定，使其清楚自身的责任和安全违规的后果。

二、对信用平台重要安全区域采取隔离控制，禁止未授权的外部人员出入。

三、禁止外部人员携带与工作无关的具有录音、录像、拍照、信息存储等功能的设备进入信用平台重要安全区域。

四、对所有进入信用平台重要安全区域进行维修、服务、参观等的外部人员进行全程旁站陪同。