天津市红桥区信用信息共享平台
安全运行管理制度
（试行）

第一条 信用平台监督检查

一、领导小组办公室负责组织信用平台监督检查工作。人员管理、教育相关检查由主管人事部门具体执行，安全技术相关检查由各工作小组具体执行。

二、监督检查内容包括各项信息系统技术措施有效性和安全管理制度执行情况。

三、安全管理员应定期（每月）全面检验信用平台在运行中的状态，防止危险状态发生，并根据可能的危险状态制定防范和处理措施。

四、安全管理员应定期（每年至少两次）对信用平台进行安全性能检测，采用漏洞扫描、模拟攻击等安全监测手段对不同网段进行安全测试，并出具安全检测报告；对发现的安全威胁，提出整改意见，经领导审批后，负责人员监督落实。

五、业务操作人员应审查业务处理过程和结果，发现问题应及时查明原因。对不能确认的异常现象，必须向市信息中心报告。

六、对计算机信息系统安全运行的监测记录及其分析结

果应严格管理，未经市信息中心许可不得对外发布或引用。

第二条 信用平台安全审计

一、安全审计主要指记录和跟踪信用平台状态变化，监控、记录对程序和文件的使用以及对文件的处理过程等。安全审计管理指利用信息系统审计方法，对信用平台进行详尽审计，对于发现的安全问题，及时通知安全管理员调整安全策略，从而达到降低安全风险的目的。

二、由安全审计员定期对信息系统的服务器、网络设备、安全设备、存储设备、应用系统进行安全审计，并形成审计记录。

三、信用平台日志内容应提供足够的信息，以便确定事件的来源和结果，日志包括以下内容：事件发生的时间、地点、类型、主体、客体和结果（成功或失败）等。

四、信用平台日志存储：

1、有充足的日志存储空间，防止由于存储空间不足造成日志丢失；

2、具有存储空间阀值设置功能，当存储空间达到阀值时及时进行告警；

3、审计系统出现异常时，保证存储的日志不被破坏；

4、日志至少保存一年；

5、日志存储空间将满时，覆盖最早存储的日志数据或转

存日志数据。

五、信息系统日志的查阅及保护:

1、安全审计员定期对日志进行审查或分析，发现可疑行为及违规操作后采取相应的措施，并及时报告;

2、提供对日志的统计、查询功能，包括按时间范围、主客体身份、行为类型等条件进行检索查询;

3、安全审计员调阅、备份、删除日志，必须进行记录;

4、对审计系统和审计信息进行访问控制，保证日志不被篡改、伪造和非授权删除。

六、系统管理员必须定期查看并校对系统时钟，确保审计日志中事件发生时间记录的准确性。

第三条 恶意代码防范管理

一、安全管理员和系统管理员共同负责信用平台恶意代码防范工作：规划防范策略，经审定后组织实施；及时关注恶意代码预警信息，妥善调整防护策略；检测、记录所采取的防范操作。

二 、所购买和使用的恶意代码防范产品必须是经过国家相关主管部门认可、认证的产品。

三、本单位所有计算机必须安装领导小组办公室指定的杀毒软件，不得私自卸载。

四、定期对恶意代码库进行升级，恶意代码库加载工作

由安全管理员负责。

五、信用平台工作人员遇到恶意代码发作，应立即断开网络连接，及时清除恶意代码；无法清除的由领导小组办公室辅助处理。彻底解决后，方可重新入网。

六、所有移动存储介质在使用前，都必须进行恶意代码查杀工作，确保其无恶意代码。需使用的各种软件，安装前应进行恶意代码查杀。

七、重要资料除在非系统盘存储外，还应利用移动存储介质备份，以防遭恶意代码破坏而遗失。信息的备份及其介质管理按有关规定执行。

八、安全审计员负责对恶意代码防范措施的落实情况进行监督检查。

第四条 安全漏洞与补丁安全管理

一、系统管理员和安全管理员应及时掌握信用平台安全漏洞预警信息，并采取加载相关补丁、关闭系统端口、调整防火墙防护策略等措施提高系统安全防护能力。

二、紧急补丁必须在一天内、重要补丁必须在一周内、一般补丁必须在两周内完成补丁的测试、发布和加载工作。

三、补丁加载之前必须经过恶意代码查杀和测试，做好应用系统和关键数据的备份工作。

四、补丁加载工作由系统管理员负责操作，安全审核员

负责检查，遵守补丁加载流程。

五、建立健全补丁分发管理机制，对信用平台补丁使用情况进行实时监管。

第五条 信用平台边界防护策略

一、系统管理人员应屏蔽与信用平台无关的所有网络功能，防止非法用户的侵入。

二、实现信用信息数据的合法合理的流转，每个不同的接入点只能访问到需要访问的资源，严格控制对核心区域和数据的访问，关闭所有不必要的服务和非法 IP。

三、系统边界处应启用抗 DDOS 攻击和抗扫描等安全功能，进一步保护网络最大限度的不受攻击的影响。

四、通过策略路由功能实现内网 IP 对互联网的访问。

五、通过安全网关软件限制功能智能跟踪软件的特征码，根据事先定义的策略智能实现软件的限制。

六、根据不同的 IP 组对带宽的不同需求制定不同的带宽管理策略。

七、 禁止多种知名蠕虫病毒进行传播。

八、通过内网管理功能监控每个 IP 的流量和并发连接数，根据这些数据快速判断哪些 IP 中了蠕虫病毒或 ARP 病毒、哪些 IP 在正常使用，从而快速定位和解决网络问题。

九、定期查看边界防护访问日志，及时发现攻击行为和

不良的上网记录。

第六条 信用资源访问策略

一、为保证信息资源的安全，分别建立资源访问安全控制策略，包括管理员权限管理策略、用户查询权限管理策略、信息资源授权策略、信息资源存储安全策略、信息资源传输安全策略等。

二、所有放置在服务器端的文档、数据以及配置信息均为受保护信息，对相关服务器的操作均由指定的管理人员进行。管理人员根据工作流程，按照需求对使用人员进行授权，授权通常包括对相关数据及文档的访问范围、许可的操作方式、有效时间界定等。

三、获得授权的人员不得将自己获得的数据、文档或访问信息传播给非授权用户。

四、严禁所有未经授权，对数据库服务器系统以及计算机系统进行访问或操作的行为。