# 天津市红桥区信用信息共享平台
# 数据安全规范
# （试行）

## 第一章 总述

### 第一条 试用范围

本标准规定信用信息平台数据的安全保障要求和监管要求。

本标准适用于信用信息平台数据的保护，也可用于第三方安全服务机构开展信用信息平台数据安全保障服务的指导。

### 第二条 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 5271.1-2000 信息技术 词汇 第1部分:基本术语

GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求

GB/T 25069-2010 信息安全技术 术语

# 第二章 数据安全保障要求

## 第三条 概述

信用信息平台数据安全保障要求包括数据防护强度要求、数据保密强度要求、数据备份强度要求。

## 第四条 数据防护强度

一、认证方式。应采用密码+动态验证码认证方式，提供数据访问的有效控制，密码应包含数字、字母、特殊符号，密码长度应不低于12位，密码应定期修改；

二、数据访问。应采用授权及身份认证的方式，其中第三方证书应由权威可信机构颁发，提供数据访问者鉴别；应采用安全的访问通道，保障对数据的安全访问，如通过web访问数据时，应提供VPN安全隧道；

三、权限管理。应采用基于用户组或角色的方法，进行用户组、角色的统一创建、管理、权限分配，保障主体访问数据的权限边界；

四、数据隔离。应对平台不同类型数据进行逻辑隔离，不同隔离域应具有不同访问操作权限；

五、数据传输。应采用安全措施保证数据传输安全；数据传输中数字摘要应符合国家密码算法相关规定，保障数据的完整性；能够对简单的完整性错误进行检测和恢复；

六、数据销毁。采用消磁、高级清零或多次复写等方式在用户要求删除数据或设备在弃置、转售前将其上所有数据彻底删除，并无法复原；

七、数据监控。应提供数据的基本监控手段，如通过数据的监控，可获取数据的历史访问活动。

## 第五条 数据保密强度

一、存储方式。平台数据存储应符合国家密码算法相关规定，密钥长度应不低于128位，对涉及个人隐私的重要数据如个人身份信息等密钥长度应不低于256位；

二、敏感标记。应对信用信息平台中涉及个人隐私的重要数据，进行敏感标记，避免相关敏感数据的泄露；

三、脱敏处理。应对信用信息平台中敏感标记的数据按照脱敏规则进行数据脱敏处理，实现敏感隐私数据的可靠保护；

四、隐私保护。应明确数据隐私保护范围和要求；

五、设备安全。应采用存储设备保护技术，保障承载数据设备的安全，并应确保未授权恶意用户无法读取设备内容。

## 第六条 数据备份强度

一、备份恢复。应提供本地数据备份与恢复功能，数据应每天增量备份，完全数据备份至少每周一次，备份介质场外存放；

二、热备数量。采用双机热备份，保障数据被破坏时，应可实时恢复；

三、容灾。采用异地备份方式容灾；

四、冗余。应采用冗余技术设计网络拓扑结构，应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统高可用性；

五、虚拟机迁移。当信用信息平台部署在虚拟机上时，承载数据的虚拟机系统应具备高可用性，当虚拟机出现异常时，可通过自动迁移技术在其他宿主系统上运行；

六、备份测试。应定期检查和测试备份介质的有效性，确保可用性。

## 第七条 数据安全监管要求

一、日常监测要求

（一）应对通信线路、主机、网络设备和应用软件的运行状况、流量、用户行为等进行监测和报警，形成记录并妥善保存；

（二）应根据监测指令对信用信息平台的双向数据流进行监测，对发现的不良信息进行记录，形成监测日志，重大问题及时上报给有关部门；

（三）应根据过滤指令对信用信息平台的双向数据流进行过滤，对发现的不良信息进行过滤处置，并进行记录，形成过滤日志，重大问题及时上报有关部门；

（四）应定期对监测和报警记录进行分析、评审，发现可疑行为，形成分析报告，并采取必要的应对措施；

（五）应对设备状态、恶意代码、补丁升级、安全审计等安全相关事项进行统一管理；

（六）应对系统数据的使用进行预测，以确保充足的处理速度和存储容量；

（七）应对通过平台面向公众发布的信息内容实时安全监控，并进行日志留存；

（八）应对用户进行审计，全程记录使用行为；

（九）应定期对运行日志和审计数据进行分析，以便及时发现异常行为；

（十）应具备对分布式拒绝服务攻击的监测与过滤能力。

二、安全审计要求

（一）应对以下事件生成审计日志：

1、管理员和用户鉴别；

2、管理员和用户的操作行为；

3、网络访问控制，包括平台、主机和数据库的远程连接、远程操作、远程数据传输。

（二）审计日志应包括事件类型、事件时间、事件主体、事件客体、用户IP、事件成功/失败、事件详细信息等字段；

（三）平台内应设置统一的时钟源，并确保平台各信息设备时间与时钟源同步，从而保证安全审计记录中事件时间的准确性；

（四）应提供审计日志的可选择查询功能，支持按以下条件之一或组合进行查询：事件类型、事件时间、触发事件用户、事件主体等；

（五）应保护审计日志不被未授权访问、修改和破坏；

（六）审计日志存储设备应采取相应措施，保证审计日志不丢失；

（七）应提供对审计日志的统计、查询、分析、生成审计报表、导出和清空等功能。

三、定位溯源要求

（一）应具备数据定位溯源技术能力，准确定位存在信息安全问题的应用或服务的源头，并保存相关记录，及时上报有关部门；

（二）应启用数据溯源机制，对非溯源数据进行警示；

（三）应具备出现问题后可以立即启用溯源的技术手段，确保溯源的及时有效。

四、日志留存要求

（一）应根据监测指令和过滤指令对信用信息平台的数据流进行监测，形成监测日志和过滤日志；

（二）监测日志和过滤日志记录应至少包括源/目的IP、物理地址、源/目的端口、不良信息、采集时间以及触发监测动作的监测指令标识等；

（三）日志留存应不少于六个月，对超过六个月的日志通过存储介质备份；

（四）应提供日志查询功能，可依据时间、IP地址、URL等进行独立或条件组合查询；

（五）日志留存的信息存储应与其他业务系统有效隔离；

（六）应记录系统管理员的操作日志，日志记录应至少包括：操作用户、操作时间、操作用户IP地址、操作用户物理地址、操作内容等，并定期对操作日志进行审计；

（七）应对平台中的用户信息、日志信息等负有保密义务，不得出售、篡改、伪造、删除、泄露或违法使用用户信息及日志信息。

五、应急处置要求

（一）应建立信用数据应急处置机制，建立相应的应急处置技术能力，并编制应急处理方案，以对存在信息安全问题的数据、应用或服务及时处理；

（二）在紧急情况下，应能够停止全部或部分服务，并保存相关记录，及时上报有关部门。