

天津市公共信用中心文件

津信用〔2020〕6号

关于印发天津市信用信息共享平台数据安全 管理暂行办法的通知

各部门：

《天津市信用信息共享平台数据安全管理办法》已经中心主任办公会审议通过，现印发你们，请遵照执行。

2020年8月31日



天津市信用信息共享平台数据安全管理办法

第一条 为了确保天津市信用信息共享平台的数据安全，使得在信息系统使用和维护过程中不会造成数据丢失和泄密，特制定本制度。

第二条 本制度适用于天津市信用信息共享平台的所有管理者、运营者和使用者。

第三条 计算机信息系统必须使用正版软件，并及时进行系统升级或更新补丁；计算机信息系统必须装有防毒杀毒软件，并定期进行病毒检验；与互联网相联的计算机信息系统要有防止非法入侵措施。

第四条 天津市信用信息共享平台必须有全面、规范、严格的用户管理策略或办法。系统管理员账号专人保管，专人使用，定期更改密码。系统管理员对用户实行集中管理，对用户按职能分组管理，设定用户访问权限，严禁跨岗位越权操作；严防非法用户或非授权用户对非授权服务、数据及文件的访问、使用和修改等。对用户身份、主机身份、事件类型等应进行安全审计，并留存审计日志，审计日志应进行妥善保存。

第五条 计算机信息系统与数据库主机必须建立在正规机房，机房要在场地面积、用电环境、使用环境、消防防雷等方面符合国家有关规定。

第六条 天津市信用信息共享平台中的每个分平台每年要进

行一次等保三级测评，按照测评要求及时修正，确保满足国家等保三级的安全要求。

第七条 对数据的各项操作实行日志管理，严格监控操作过程，对发现的数据安全问题，要及时处理和上报。

第八条 强化对自然人敏感数据的安全保护，涉及自然人数据只有系统管理员在获得相关主体的授权后，方可查询，查询记录记入日志，全程可追溯。其他任何权限用户不得进行查询。

第九条 未经批准，系统管理员不得直接对后台数据库进行数据更改操作，确需后台操作的，必须上报分管领导批准，并事先对数据库进行备份后进行，同时，详细记录操作过程及数据更改情况存档备查。

第十条 存放备份数据的介质必须具有明确的标识。备份数据必须异地存放，并明确落实异地备份数据的管理职责。

第十一条 注意计算机重要信息资料和数据存储介质的存放、运输安全和保密管理，保证存储介质的物理安全。

第十二条 任何非应用性业务数据的使用及存放数据的设备或介质的调拨、转让、废弃或销毁必须严格按照程序进行逐级审批，以保证备份数据安全完整。

第十三条 数据恢复前，必须对原环境的数据进行备份，防止有用数据的丢失。数据恢复过程中要严格按照数据恢复手册执行，出现问题时由技术部门进行现场技术支持。数据恢复后，必须进行验证、确认，确保数据恢复的完整性和可用性。

第十四条 数据清理前必须对数据进行备份，在确认备份正确后方可进行清理操作。历次清理前的备份数据要根据备份策略进行定期保存或永久保存，并确保可以随时使用。数据清理的实施应避开业务高峰期，避免对联机业务运行造成影响。

第十五条 需要长期保存的数据，数据管理部门需与相关部门制定转存方案，根据转存方案和查询使用方法要在介质有效期内进行转存，防止存储介质过期失效，通过有效的查询、使用方法保证数据的完整性和可用性。转存的数据必须有详细的文档记录。

第十六条 天津市信用信息共享平台的所有使用和维护人员都应签署安全保密协议，如有违反协议的行为将依法追究相关人员的责任。

第十七条 非本单位技术人员对本单位的设备、系统等进行维修、维护时，必须由本单位相关技术人员现场全程监督。计算机设备送外维修，须经设备管理机构负责人批准。送修前，需将设备存储介质内应用程序和数据等涉经营管理的信息备份后删除，并进行登记。对修复的设备，设备维修人员应对设备进行验收、病毒检测和登记。

第十八条 管理部门应对报废设备中存有的程序、数据资料进行备份后清除，并妥善处理废弃无用的资料和介质，防止泄密。

第十九条 运行维护部门需指定专人负责计算机病毒的防范工作，经常进行计算机病毒检查，发现病毒及时清除。

第二十条 本制度自印发之日起执行。

天津市公共信用信息中心 第十二页

天津市公共信用信息中心

2020年8月31日印发
