

青浦区大数据中心网络与信息系统账号与密码管理制度

第一章 总 则

第一条 为进一步加强网络与信息系统的账号与密码使用管理，有效提升安全防护能力，确保系统数据安全，依据相关规范要求，紧密结合自身实际，制定本管理制度。

第二条 本管理制度适用于青浦区大数据中心拟建、在建以及在线的非涉密信息系统和网络设备、服务器、数据库、安全产品等账号与密码管理。

第二章 日常管理

第三条 账号的分配权限和开设范围应严格遵循最小化原则，即分配能满足工作要求的最小权限，另外可以拥有账号的人群应限制在最小范围以内。

第四条 每一账号仅对应一人拥有，确保用户身份标志的唯一性，并拥有不同的权限级别。不同用户的登录操作在日志文件上均有记录，便于追查问题。

第五条 管理员按照工作需求拥有相应的用户权限，管理员不得擅自开放权限至不同用户。

第六条 密码应由字母、数字及特殊符号组成，长度不少于8位，从而提高密码安全强度。

第七条 用户密码需按照用户角色和权限要求定期更新，确保周期内密码的安全性。系统管理用户和主要业务用户密码做到月度更新，一般用户密码做到季度更新，且更改后的密码不能与曾经使用过的密码相同或类似。

第三章 使用管理

第八条 工作人员应保证密码安全，不得向其他任何人泄漏。对于泄漏密码造成的损失，由账号使用本人负责。

第九条 用户忘记密码时，管理员必须在对该用户进行适当的身份识别后方可实施账号密码初始化操作。

第十条 密码不得以任何形式存放于可公共访问的设备中；密码不得以明文方式存放于任何电子存储介质中；密码建议不记录在传统介质（如纸张）中，如确需记录，则记录介质必须妥善保存。

第十一条 当发生以下情况时，管理员应立即取消账号或更改密码，并做好记录：

- （一）系统临时运维服务商维护完成；
- （二）账号使用者离开岗位；
- （三）账号使用者由于工作内容变动不再需要访问权限；
- （四）账号使用者违反了有关密码管理规定；
- （五）有迹象表明密码可能被泄露；
- （六）发生其他情况，上级管理人员认为不应再具有访问权限的。

第四章 附 则

第十二条 本管理制度的解释权和修改权归青浦区大数据中心所有。

第十三条 本管理制度自发布之日起施行。

青浦区政务服务办公室

2022 年 11 月 17 日