技术部安全管理规范

第一章 总则

第一条 为了加强对技术部业务内部管理，提高技术部门工作安全、效率和质量，依据公司规章制度等相关政策，制定本管理制度。

第二条 本制度适用于公司技术部门。

第二章 计算机安全管理规范

第三条 必须明确每台计算机终端的责任人。

第四条 所有计算机必须安装防病毒软件，防病毒软件由公司统一采购或指定。

严禁擅自安装和使用上网代理类、黑客性质类、网络和通讯管理类的危害信息安全和网络安全的软件。

第五条 计算机的使用要保持清洁、安全、良好的计算机设备工作环境，禁止在应用环境中放置易燃、易爆、强腐蚀、强磁性等有害计算机设备安全的物品。

第六条 非本部门技术人员对本部门的设备、系统等进行维修、维护时，必须由本部门技术人员现场全程监督。计算机设备送外维修，须经负责人批准。

第七条 不得使用任何方法窃取他人计算机口令，非法入侵他人计算机系统。

第八条 计算机不得一直处于“共享”状态，如需要共享时，必须设置密码，设定用户权限，用完即刻取消共享。

第九条 计算机用户严禁下载和使用未经测试、来历不明的软件，未经病毒查杀不得使用U盘等介质。

第三章 源代码安全管理制度

第十条 做好所有公司源代码安全管理工作，对于所有接触源代码的各部门和各岗位做好源代码管理工作。源代码包括公司开发人员自行编写实现功能的程序代码、相应的开发设计文档和使用过的第三方软件、控件和其他支撑库等。

第十一条 所有系统的源代码均必须及时加入到指定的源代码服务器中的SVN库中。

功能开始编写或者调整代码之前，相应的设计文档必须加入SVN库，可以指定专人负责检查工作。

所有提交到SVN上的代码必须保证编译通过，而且提交的时候不会影响主干其他程序的正常运行。

系统开发或代码调优结束后，提交测试人员测试之前，相应的源代码必须提交到SVN库。

第十二条 源代码服务器对于共享的SVN库基于身份和口令进行访问授权，在SVN库中设置用户，并为不同的用户分配不同的适合工作的最小访问权限，严格控制用户的读写权限，应以最低权限的原则进行分配权限，如果开发人员不需要对相关系统源代码做更新是，需及时删除账号。

工作变化后要实时回收用户的相关权限，每个普通用户切实保证自己的用户的身份和口令不泄露，用户要经常更换自己在SVN库中的账号和口令。

对SVN库要求建立专人管理制度，任何其他人不得在未获得相关领导授权的情况下操作和使用此设备，此设备专用人也不得私自同意或者漠视他人在非获得授权的情况下使用此设备。

SVN库设备不得转做他用，通过网段隔离的方式使此设备是能在技术部门局域网中使用，并保证其他网段不能访问，外来设备不得直接连接到此设备上，如果需要拷贝文件，必须在相关领导的监督之下进行。

第十三条 项目开发或实施期间，所有参与研发人员，每日下班前必须讲当日源代码提交至SVN库，每一次提交对所提交内容做好注释，所提交代码必须是编译无错误版本。

如不能链接到公司服务器，需要跟技术部门负责人沟通确认后可以以拷贝等别的方式进行代码上传。

1. 所有员工在公司工作期间所开发软件产品（项目）源代码所有权以及版权归公司所有，严禁公司员工私自将源代码散发给他人（包括公司其他与工作无关人员），技术部员工要做好源代码保护工作，避免代码泄露，凡违反以上规定，导致造成公司损失，公司将依法追究相关人员责任并要求赔偿公司损失。

 如需向公司以外人员提供源代码，必须以书面的形式提出申请，在申请中必须说明对方所在公司、人名以及原因等信息，经批准后由部门负责人将制定的源代码提供给对方。

第四章 数据安全管理制度

第十五条 做好所有公司系统的用户账号、密码管理工作，密码应设置成复杂密码，应包含数字、字母、大小写等，并定期更换。

对维护和运维的系统应制订可行的备份和灾难恢复方案，以保障在系统故障、或数据丢失时及时恢复业务系统数据。

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。

第十六条 注意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。

数据恢复前，必须对原系统的数据进行备份，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，出现问题时由设备厂商进行现场技术支持。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。

数据删除前，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。数据删除的实施应避开业务高峰期，避免对联机业务运行造成影响。

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。

需要长期保存的数据，根据转存方案和查询使用方法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。