文档密级：C

源代码管理规范

一、 总则

1. 目的

为有效控制管理源代码的完整性、可用性、保密性，确保其不被非授权获取、复制、传播和更改，明确源代码控制管理流程，特制定此规范。

2. 适用范围

本制度适用于所有涉及接触源代码的各岗位，所涉及人员都必须严格执行本管理办法。

3. 职责

源代码直接责任管理部门为信息技术部。本办法管理重点在于控制管理源代码的完整性，不被非授权获取，不被非授权复制和传播。本规范所指源代码不仅限于公司开发人员自行编写实现功能的程序代码，而且还包括相应的开发设计文档及用于支撑整个平台系统运行所必须具备的第三方软件、控件和其它支撑库等。

二、 管理细则

1. 源代码完整性保障

（1） 所有软件的源代码及相应的开发设计文档均必须及时加入到公司内部 GITLAB 库中。

（2） 我们研发的产品软件运行所必须的第三方软件、控件和其它支撑库等文件也必须及时加入到公司内部的 GITLAB 库中。

（3） 软件开始编写或者调整代码之前，其相应的设计文档必须签入 GITLAB 库。软件编码或功能调整结束提交测试部门测试验证之前，相应的源代码必须签入 GITLAB 库。

（4） 技术支撑部门对代码的测试时必须从公司内部源代码 GITLAB 库中获取代码，包括必须的第三方软件、控件和其它支撑库等文件，然后进行集成编译测试。

2. 源代码的授权访问

（1） 源代码服务器对于共享的 GITLAB 库的访问建立操作系统级的，基于身份和口令的访问授权。

（2） 在 GITLAB 库中设置用户，并为不同用户分配不同的权限，权限应按工作的最小访问权限。且源代码库中不可有共享账号存在。

（3） 要求连接 GITLAB 库时必须校验 GITLAB 中用户身份及其口令。在 GITLAB 库中要求区别对待不同用户的可访问权、可创建权、可编辑权、可删除权、可销毁权。严格控制用户的读写权限，应以最低权限为原则分配权限；开发人员不再需要对相关信息系统源代码做更新时，须及时删除账号

（4） 工作任务变化后要实时回收用户的相关权限，对 GITLAB 库的管理要求建立专人管理制度专人专管。每个普通用户切实保证自己的用户身份和口令不泄露。

（5） 用户要经常更换自己在 GITLAB 库中账号的口令，且口令需满足公司安全需求，不可设置弱口令。

（6） 涉及存储、使用、编辑源代码的计算机必须建立专人专用制度，并且对计算机进行受控保护,具体参照公司《信息资产管理规范》和《终端安全管理规范》执行。

（7） 曾经涉及、触及源代码的计算机在转作它用，或者离开研发部门之前必须由安全人员全面清除计算机硬盘中存储的源代码。如果不能确定，必须对计算机中所有硬盘进行全面格式化后和覆盖，方可以转做它用。

（8） 外来存储设备不得直接连接到研发部门的计算机设备上。如需拷贝文件，必须通过统一的研发部指定的公用计算机上在网管人员监督之下进行。此公用计算机在任何时候不得接触、访问、存储源代码文件。

（9） 通过网段隔离方式使研发部的计算机只能自行组成局域网，并保证其它网段不能访问到研发部的网络和网络中的计算机设备。

3. 源代码复制和传播

（1） 任何源代码文件包括设计文档等技术资料不得利用如 QQ、微信、MSN、邮件或上传 Github 平台等涉外网络环境形式进行传输。

（2） 源代码向研发部门以外复制必须获得总经理的书面授权。并必需记录复制人、批准人、复制时间、复制目的、文件流向、文件版本或内容。

（3） 源代码以任何介质形式进行存储的备份，必须由专人负责保管。对于这些介质地借阅，用于研发部内部使用的必须获得研发部负责人的授权，对于用于研发部以外使用的必须获得总经理的书面授权。

（4） 对于以纸质形式存在的源代码清单、设计文档等，需进行专人管理。对于这些纸质材料的外借、分发、复印等，只要非研发部门内部使用的情况均必需获得总经理的书面授权，对于研发部门内部使用的则必需如数按时按量回收，并且使用区域仅限于研发部门内部，对于需要离开研发部门场所的情况，同样需要获得总经理的书面授权。

（5） 对于因合作需要，需要向外复制、传播、分发源代码的，不论是全部还是部分代码和资料，均必需和对方签订技术、源码的保密协定，明确对方应当承担的对源码保密的责任和义务。

4. 源代码平台的日常管理

（1） 软件的源代码文件及相应的开发涉及文档应及时加入指定的源代码服务器的指定库中。

（2） 源代码管理平台中不得存放任何生产环境配置，包括但不限于 IP 地址、端口号、数据库密码等。

（3） 定期巡检源代码管理平台账号，清理无效或不再使用的账号，整理账号权限。

（4） 项目上线阶段检查源代码管理平台各项目的使用情况，检查内容包括但不限于硬盘空间检查、目录规范性检查、归档检查。

（5） 定期巡检源代码管理平台服务器使用状况，巡检内容包括但不限于服务器性能检查、定期备份检查、服务器安全性检查。

（6） 定期进行源代码管理平台漏洞检测及各类补丁版本维护。

（7） 源代码管理平台不得对互联网开放。

三、 附则

1. 对违反上述安全管理条例的员工，依据《信息安全惩戒规范》进行处理。

2. 本制度由公司信息安全局负责解释和修订。

3. 本制度自发布之日起开始执行。