文档密级：C

终端安全管理规范

一、 总则

1. 目的

为加强公司内部 IT 终端安全管理工作，确保 IT 设备安全正常运行，保障公司重要信息资产的安全，防范系统风险，规范 IT 终端的使用行为，特制订本管理制度。

2. 范围

本管理制度适用于公司所有员工及第三方人员对 IT 终端设备的使用和管理，包括台式机、笔记本电脑、移动存储介质、打印机、扫描机等 IT 设备及安装在其上的系统的使用。

3. 职责

信息技术部：

（1） 对 IT 设备的使用和管理进行统筹规划。

（2） 负责 IT 设备的日常管理和维护。

（3） 对违反本制度的行为及时教育和纠正。

设备使用者：

（1） 在日常的 IT 设备使用和操作中严格遵守公司的各项管理规定。

（2） 在 IT 设备使用和操作中，如果发现异常情况，应及时与信息技术部联系，出现重要情况须立即汇报。

（3） 配合信息技术部的日常管理工作，接受信息技术部对 IT 设备的维护及监管。

（4） 有义务向信息技术部或其他有关部门报告违反公司相关规定的行为。

部门负责人 ：

（1） 以身作则，率先达到本规范的要求，起到表率作用。

（2） 对本部门员工的执行情况进行约束和管理。

（3） 对违反规定的行为进行批评教育。

二、 管理细则

1. 设备安全管理

（1） 未经许可，员工不得携带私人计算机设备进入公司办公场所。

（2） 访客、第三方合作伙伴、厂家工程师等带入公司办公场所的私人计算机设备必须在信息技术部备案后方可使用。

（3） 公司所有计算机设备必须加入到公司域环境中，并采用域账号登录系统。

（4） 公司所有计算机设备必须杀毒软件 McAfee。

（5） 计算机设备必须有严格的口令访问控制措施，口令设置需满足公司安全策略要求。

（6） 离职、离岗或其他原因回收的员工的计算机设备。应统一交由基础架构局进行数据清除处理后，再发放其他员工。

（7） 未经信息技术部许可，禁止私自拆卸计算机设备。

（8） 计算机设备丢失或被窃后应及时报告部门负责人和部门资产管理员。

2. 网络使用管理

（1） 禁止使用 P2P 等下载软件，如电驴、BT、迅雷等软件。

（2） 禁止私设网络，扰乱公司正常网络运行，一经发现将没收相关网络设备。

（3） 禁止危害他人的隐私安全。

（4） 访问网络应遵守国家相关法律法规。

（5） 公司内的网络接入服务，只能用于工作目的，公司有权对员工网络上的行为进行监管。

（6） 禁止利用公司网络或其它资源，炒股、游戏、观看电影等和工作无关的行为。

（7） 禁止利用公司网络接入服务发送或者转发虚假、黄色、反动信息。

（8） 禁止利用公司网络接入服务发送或者转发宣扬个人政治倾向或者宗教信仰。

（9） 禁止将公司受控级别和更高级别的保密信息上传到公众论坛、网盘等公共资源服务。

（10） 所有通过网络发送的保密信息都必须有明确的接收人，而且是公司业务所必需的，且遵循《信息资产管理制度》的相关规定。

（11） 对于违反公司规定、造成公司损失的行为，公司有权追究其相关责任。

3. 公司邮件使用管理

（1） 公司邮箱只能用于公司目的，公司有权对所发送的内容进行监管。

（2） 禁止利用公司邮箱发送或者转发虚假、黄色、反动信息。

（3） 禁止利用公司邮箱发送或者转发宣扬个人政治倾向或者宗教信仰。

（4） 禁止利用公司邮箱发送或者转发垃圾信息。

（5） 发送邮件必须有清楚的主题，发送前须再次确认收件人员是工作范围必需知晓此邮件的人员。

（6） 员工必须以本人的真实身份使用用于办公用途的邮箱，禁止以他人名义滥发邮件或盗用他人邮箱。

（7） 未经授权任何人不得尝试以他人账户口令进行登录，阅读他人邮件内容。

（8） 邮箱用户的登录口令，必须严格保密，不得泄露，如将其借予他人使用，由此造成的一切安全后果由邮件账号所有人承担。

（9） 员工不要阅读和传播来历不明的邮件及附件，提高邮件病毒的防范意识，避免传递病毒邮件。

（10） 员工不得将本公司提供的电子邮件地址用于非工作目的(特别是以娱乐、购物、交友等为目的身份注册)。

（11） 员工如通过电子邮件系统发送保密信息，必须遵循《信息资产管理制度》的相关规定。

4. 用户账号及口令管理，屏幕保护设置

（1） 所有终端应启用屏幕保护程序，时间为 5 分钟，并设定在恢复时使用密码保护。

（2） 员工必须妥善保管好自己的用户名和口令，严防被窃取而导致泄密。不得将个人账户/口令借/转他人使用。

（3） 禁止将口令写在纸上或记录本内。不得以明文方式将口令保存在电脑内，如果需要保存密码，必须以加密方式保存。

（4） 员工至少每 3 个月更改一次口令，避免再次使用旧口令或半年内循环

使用旧口令。

（5） 终端账号口令的最小长度为 8 位，口令必须包含大、小写字母、数字和字符至少任意三种的组合，不得设置轻易联想到的账号口令。

5. 防病毒和补丁管理

（1） 所有连接到公司网络的计算机设备必须安装公司指定的防病毒软件，不得禁用或绕过病毒保护软件。

（2） 对于防病毒软件不能自动清除并引起安全事故的病毒，须及时向信息安全局报告。

（3） 任何部门和个人在发现电脑系统中存在病毒入侵的迹象时，在及时采取有效措施的同时并立即向信息安全局报告。有效措施包括：关闭计算机、断开网络，使用防病毒软件进行扫描查杀等。

（4） 禁止使用来历不明的软件或盗版软件，禁止在未安装有效防病毒软件的情况下私自从互联网上下载软件。

（5） 使用外部文件或存储设备前应进行病毒检查。

（6） 计算机终端资产责任人应定期检查系统补丁更新情况,及时安装系统补丁。

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。