FOSUN 复星

复星集团
信息安全管理制度

[IT_001 _V3.0]

[集团数智化与 AI 条线信息安全团队、集团风控条线法务部]

Fosun Group
2024年 08 月 28 日

第一章 总则

第一条 为提高集团员工的信息安全意识，规范员工的行为，指导员工合理、安全的使用信息资产，防止有意或无意的破坏信息安全行为的发生，提高集团整体信息安全水平，根据集团现有状况，制定本制度，以此明确集团信息安全管理要求及员工日常工作规范。同时，集团建立并持续完善信息安全体系，识别和评估业务的信息安全风险，实施应对和缓解策略，以最小化信息安全风险。鉴于信息安全风险的动态变化，集团将持续完善本制度，以确保其有效性和适应性。

第二条 本制度适用于上海复星高科技（集团）有限公司及其直接或间接管理、控制的子、孙公司以及各分公司（以下统称集团）的所有部门、所有员工和能接触到信息资产的第三方人员。

第二章 声明

第三条 员工的工作计算机、工作手机、工作电子终端、工作电子邮件系统及集团内部网络等 IT 设备及信息系统仅可用于工作用途，应当仅存放工作相关的信息。禁止利用集团 IT 资产（包括集团派发的计算机、手机、工作电子邮箱等）处理个人事务，以避免集团在信息安全管理中触及个人隐私，任何员工不应对在该等设备或信息系统中储存或传输的信息存在任何隐私侵权。

第四条 员工利用集团的资产所产生、处理和存储的一切信息资产，其所有权归集团拥有。集团有权对该等信息资产进行收集、监控、处理或删除。

第五条 集团管理信息资产，以确保在整个生命周期数据的安全性、准确性和一致性。集团出于对运营管理、安全管理和司法调查取证等需要，集团管理部门有权利在未通知员工及不需要获得员工授权的情况下，对集团 IT 资产进行监控、回收、复制、披露、使用和删除；在怀疑集团资产被攻击、破坏、泄露时，集团有进行拦截、删除、封锁及任何保护集团资产的权利，如发现集团人员有违规行为，对集团人员作出相关处罚或法律追究。

第三章 组织架构

第六条 集团信息安全管理组织架构包括：

（一） 集团安全管理委员会

（二） 集团信息安全管理组

（三） 集团安全推动组

（四） 运维执行组

第七条 组织成员与职责：

（一） 集团安全管理委员会：

1、由集团总部技术领导及成员企业各技术条线负责人担任；

2、负责监督及协调推动集团信息安全管理规范在公司内部的落地执行；

（二） 集团信息安全管理组：

1、由集团数智化与AI条线信息安全团队组成；

2、负责制定、解释、修改集团信息安全管理制度、技术规定、应急预案等，其他相关部门应按照相应的条线管理制度落实；

3、负责对接成员企业，推动信息安全管理要求在成员企业内部落地执行；监督成员企业信息安全管理执行度；

4、负责汇总整理集团和成员企业内部信息安全状况、安全事件等相关报告并报送集团安全管理委员会；

5、组织对重大的信息安全工作制度和技术操作策略进行审查，拟定信息安全总体策略规划，并监督执行；

6、组织信息安全工作检查，分析信息安全总体状况，提出分析报告和安全风险的防范对策；

7、跟踪先进的信息安全技术，组织信息安全知识的培训与考核和宣传工作；

8、制定与更新集团网络与信息系统的安全应急策略及应急预案；

9、每年组织对信息安全应急策略和应急预案进行测试和演练；

（三） 集团安全推动组：

1、由各成员企业至少指定一名信息安全接口人担任；

2、负责推动本单位执行集团信息安全要求；

3、负责上报本单位发现的信息安全事件至集团安全执行组；

（四） 运维执行组

1、由运维团队负责人及运维人员专责担任；

2、负责网络的运行管理，实施网络安全策略和安全细则；

3、负责在系统开发建设中，严格执行系统安全策略，保证系统安全功能的准确实现；

第四章 工作环境安全

第八条 应遵守安全区域访问规定，进出非授权区域时，需按照集团相关规定经相关责任人批准。

第九条 员工应安全保管身份识别证件，丢失后及时向发证部门报告，禁止将身份识别证件借与他人使用；调离集团时，应主动交还集团配发的身份识别证件。

第十条 外来人员访问办公职场，必须对访客的身份、事由的真实性与员工进行核实并进行登记。访客应在入口处由受访人员接待进入，并在职场访问期间有员工全程陪同， 进出登记表必须最少保存三年。

第五章 用户账号安全

第十一条 任何账号应依据“权限最小化”原则申请，且仅限申请账号时批准的所有者在授权范围内使用，严禁使用账号访问未授权的资源，账号所有者承担使用该账号所产生的一切责任和后果。权限审批人也应依据上述原则核实需求。

第十二条 账号正式启用前，必须为账号添加密码，所有账号密码应遵循集团密码管理要求。

第十三条 应安全保管密码，如没有可靠的物理控制措施，不要将密码写在纸上，或记录于电子文件（云笔记）中；禁止将密码在终端软件（如浏览器）上自动保存；禁止公开本人或他人的密码信息，不得猜测窃取他人账号密码。

第十四条 工作职责发生变动时，应主动申请帐号或者实物密钥权限的变更；当不再需要某系统的访问权限时，应主动申请注销账号或者权限；对不能关闭的账号或者实物密钥，应及时移交给本部门指定责任人；在离职时，应主动移交全部账号和实物密钥。

第六章 信息设备使用

第十五条 所有终端计算机应安装集团要求的桌面管理软件、防病毒软件等，员工不得自行删除或修改。

第十六条 离开座位时，应锁定或关闭计算机；应安全保管终端信息设备，周末或者节假日期间禁止将便携信息设备放在桌面上。

第十七条　禁止将集团派发的设备用于工作以外用途，原则上不要将工作设备接入办公网以外的环境，如因工作需要需与外部环境对接，再次接入办公环境时应先进行病毒的查杀。

第十八条　未经授权不得使用移动介质，经授权使用移动介质前，应进行病毒检测，确认安全后方可使用。

第十九条　未经授权不得将终端设备、移动介质、实体信息和软件等带离办公区。

第二十条　未经授权任何人不得私自调换信息设备，禁止私自拆卸、维修或者更换计算机硬件。

第二十一条　设备及存储介质提交维修、回收、报废前，应对设备上的重要数据进行备份和安全销毁。

第二十二条　应保管好个人使用的信息设备，一旦丢失，应立即向 IT 部门报告，以便及时锁定相应账号，以防止被冒用。

第二十三条　禁止未经授权为集团电脑私自连接外设，包括但不限于拨号器、无限网卡等不经过集团内部网络直接与集团外部通讯的设备、USB存储、刻录光驱、读卡器、智能手机等信息传输设备。

第七章 软件使用

第二十四条　终端设备初装或重装操作系统，必须使用集团提供的操作系统，不得随意使用其它操作系统安装包进行安装。

第二十五条　应使用集团许可的软件，禁止安装与工作无关的软件，禁止私自更改、禁用、卸载集团要求使用的软件。禁止下载或使用未经授权的盗版软件，如因员工个人使用盗版软件而引起的著作权纠纷，员工个人承担相应侵权责任，如公司因员工的侵权行为对外承担了赔偿责任，公司有权向员工追偿。

第二十六条　未经集团安全部门授权不得使用扫描软件、恶意脚本等攻击类工具对集团内网及系统进行扫描、攻击测试和干扰。

第八章 计算机网络使用

第二十七条　禁止将未经许可的计算机设备接入集团网络。

第二十八条　未经许可，不得擅自变更接入设备的网络设置。

第二十九条　禁止传播集团 WiFi 密码。

第三十条　除集团提供的互联网出口外，未经批准，在集团办公室环境不得采用任何方式（如无线网卡、调制解调器等）接入互联网或其它外部网络。经批准可以使用的，应先断开与集团网络的连接，方可连接外部网络。

第三十一条　要合法、文明访问互联网，禁止在互联网上进行违法违规活动。

第三十二条　不得滥用集团网络资源进行与工作无关的活动，如访问与工作无关的网站和互联网服务、下载与工作无关的文件、玩网络游戏、使用聊天工具等。

第三十三条　未经授权禁止有下列情况之一的计算机终端接入互联网：

（一）涉及集团绝密或机密信息的；

（二）未安装指定防病毒软件和桌面管理软件等安全管理软件、病毒库未及时更新的；

（三）经评估存在其它安全隐患，不适宜接入互联网的；

第九章 电子邮箱使用

第三十四条　严格保密自己电子邮件系统的密码，如交与他人使用，由此造成的一切后果由电子邮件账号所有人承担。

第三十五条　不得利用电子邮件服务发送与工作无关的邮件，工作邮箱内不得存放含个人隐私的任何信息。

第三十六条　严禁将集团的电子邮件用于非工作目的，特别是以娱乐、购物、交友等为目的的身份注册。

第三十七条　专用邮箱必须指定专人负责邮箱的安全使用，禁止多人共享专用邮箱权限。

第十章 数据安全管理

第三十八条　根据集团信息的价值、内容敏感程度、接触范围，敏感信息分为绝密、机密、秘密三级，以及非保密信息，由信息拥有人指定级别。当不同分类的信息汇集一起共同处理、发布或保存时，信息分类等级依据所汇集信息中最高等级来设定。

第三十九条　应及时备份工作中的重要数据，以防数据丢失；

第四十条　不得向未授权机构或人员提供集团敏感性数据（包括“绝密数据”、“机密数据”和“秘密数据”），或者未经授权将集团信息带离集团网络环境，包括拷贝至个人信息设备、发送至个人公网邮箱、上传至互联网等。

第四十一条　经授权向外部机构或人员提供敏感性数据时，必须通过数据主管理部门批准的途径和方式进行传递。

第四十二条　使用移动介质传输和存储敏感性数据时，应对数据或介质进行加密，使用结束后应及时清除介质上的敏感性数据。

第四十三条　发现存在泄露客户、员工及用户等个人信息/数据的行为，应及时向集团有关部门反馈。

第四十四条　泄露客户、员工及用户等个人隐私或个人信息属于违法行为，严禁违反集团审批流程未经授权复制、传输、公开和使用集团客户、员工及相关用户的个人信息数据。

第四十五条　不得未经授权翻印、复制、摘录和外传集团购买具有第三方版权的外部信息，信息中含有版权或者保密要求的，应严格遵照执行。

第十一章 个人信息保护

第四十六条　产业应合法合规通过自研应用程序或者第三方软件等产品收集个人信息

第四十七条　集团在使用个人信息时，仅限于为达成告知信息提供者的个人信息使用目的所必须的范围内使用；当信息使用目的发生变更时，须事先得到信息提供者本人的同意。

第四十八条　所有涉及个人信息的业务系统，应符合国家/本行业/集团规定，对未符合要求的系统需整改完成才可上线。

第四十九条　各业务系统应根据个人信息的种类、来源、敏感程度、用途等，对个人信息进行分级、分类，并采取有针对性的管理或者安全技术措施。

第五十条　信息的保存期限也仅限于必要期限内，所需期限结束后将其删除或废弃。

第五十一条　采用必要的技术手段，如加密、数据备份等，确保个人信息安全。

第五十二条　禁止任何人未授权访问和非法使用用户个人信息，如造成影响需承担相关集团处罚和国家法律法规处罚。

第五十三条　当发生个人信息泄露或流失等事故时，各公司将按照以下流程适当且迅速的对应，及时采取措施限制影响，按法律法规的要求履行义务：

（一）及时采取措施避免因事故造成损失或将损失降到最低；

（二）本公司应及时通知信息所有人；

（三）查清事故发生的原因，并应采取必要措施防止类似事件的发生；

第五十四条　对接触个人信息的管理人员、技术人员、操作人员开展相应的安全教育和培训，确保管理人员、技术人员、操作人员具备必要的知识和技能。通过内部培训、公告等方式，加强全体员工对个人信息保护的重视程度。

第五十五条　集团及各公司应定期对个人信息保护工作进行检查和评估，及时发现和纠正问题。

第十二章 防病毒要求

第五十六条　任何设备接入集团网络前，均需先安装集团规定的安全接入控制软件或防病毒软件，并进行病毒扫描，在确认该电脑安全无毒后，方可接入。

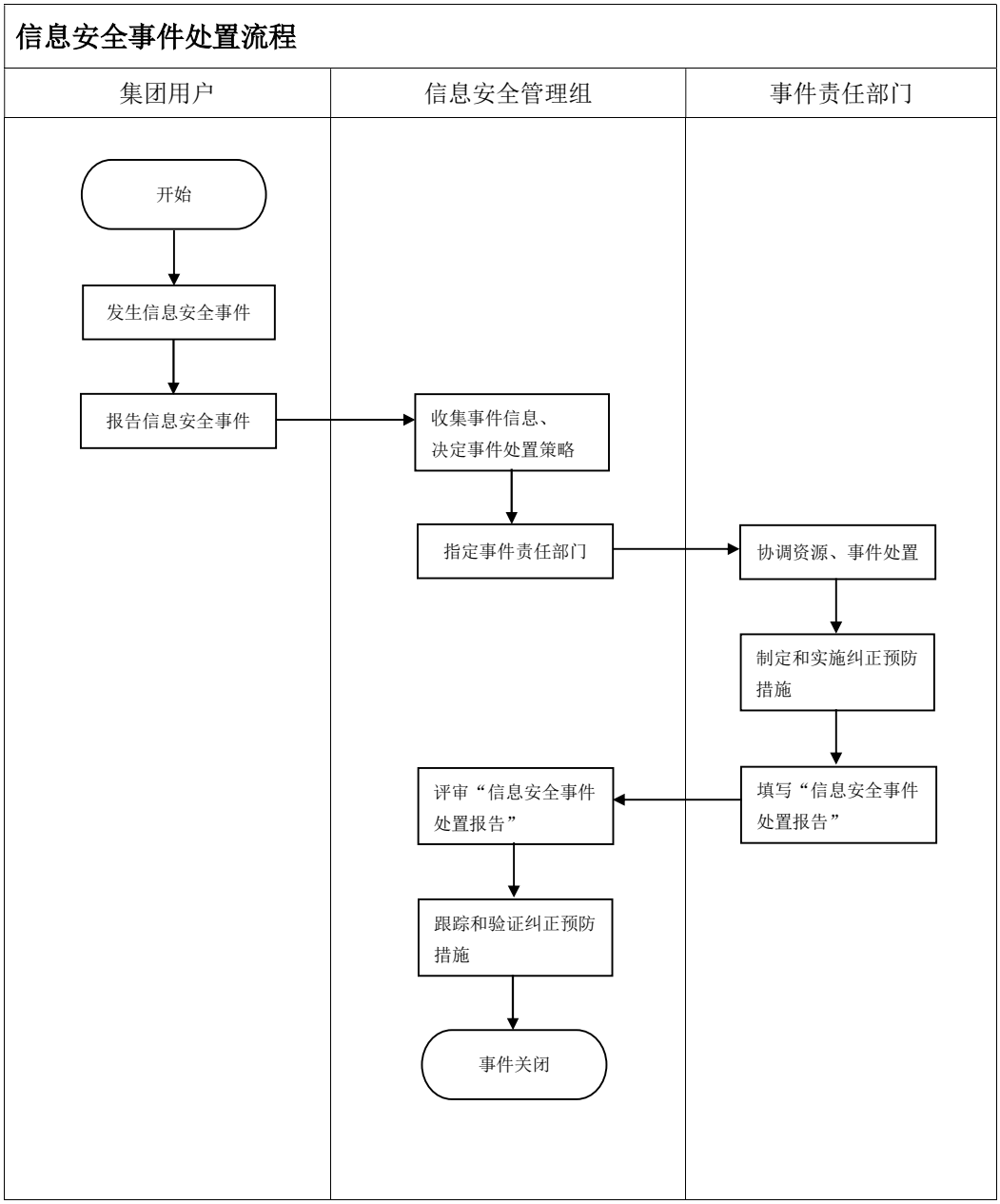
第五十七条　使用个人计算机时，要运行防病毒软件，及时更新病毒库、升级系统补丁，并定期执行病毒检测和清除。未经许可，不得下载和安装规定以外的防病毒软件或病毒监控程序。

第五十八条　使用U盘、光盘等移动介质前，要进行病毒检测，不要使用任何未经防病毒软件检测过的移动介质。

第五十九条　如发现计算机感染了病毒，或者数据被删除破坏等异常情况，要立即断开网络连接，并及时向信息安全管理人员汇报病毒情况，在得到妥善处理前不要使用被感染的文件，并保持断网状态。

第十三章 安全事件

第六十条　集团员工发现信息安全事件后，应按以下流程上报至信息安全管理组。



第六十一条　信息安全管理组收到上报情况后，应尽快制定处置策略、指定处理责任部门。

第六十二条　责任部门协调资源对事件进行处置，事件处置完成后应制定和实施纠正预防措施并填写“信息安全事件处置报告”。

第六十三条　信息安全管理组收到“信息安全事件处置报告”后，应对报告进行评估，并跟踪和验证纠正预防措施。

第十四章 处罚原则

第六十四条　对于违反以上要求及集团信息安全方针政策的行为，将按照集团的有关规定进行处罚。

第六十五条　对于违反本规范的人员，将依照情节轻重对其采取以下惩罚措施：

（一）警告提示；

（二）暂停账号或计算机终端入网，并进行通报批评；

第六十六条　对于情节严重，对集团造成重大损失，甚至构成犯罪的，交由司法机构追究其法律责任。

第十五章 附则

第六十七条　本制度由集团数智化与AI条线信息安全团队、集团风控条线法务部负责解释、修订。

第六十八条　本制度自发布之日起执行。