三一重工股份有限公司 管理制度		员工信息安全管理制度				
ZD/IT 002-2017		版本	V8	实施日期	2017 年 8 月 1 日	第 1 页 共 4 页

编制人	周碧波
审核人	李发、潘睿刚
批准人	向文波

更改记录				
标 记	处 数	更 改 依 据	更 改 人	更 改 日 期
V6	6	信息安全要求	李纪潘	2011-11-20
V7	多处	信息安全要求	肖骁	2013-8-18
V8	多处	信息安全要求	周碧波	2017-7-20

1 目的

明确员工在司或使用公司 IT 资源时的信息安全行为规范，提升员工信息安全意识，合规使用公司信息系统资源，保护公司信息资产。

2 范围

适用于三一重工所有员工日常信息安全行为规范。集团国内各事业部、各子公司等同执行；海外事业部、子公司等效执行；代理商、合资公司参照执行。

3 定义

信息安全异常：信息安全异常是指被识别的一种系统、服务或网络状态的发生，表明一次可能的信息安全策略违规或某些防护措施失效，或者一种可能与安全相关但以前不为人知的一种情况。

信息安全事件：信息安全事件是由单个或一系列意外或有害的信息安全异常现象所组成的，极有可能危害业务运行和威胁信息安全。

一级信息安全事件：有意盗窃、泄露公司保密信息，有意违反信息安全管理规定，性质严重造成重大损失。如果违反法律法规，公司依法保留追究其法律责任的权利。

二级信息安全事件：有意违反信息安全管理规定，性质严重或造成损失。

三级信息安全事件：无意违反信息安全管理规定，造成公司损失；或者有意违反信息安全管理规定，但性质不严重且没有造成严重损失。

四级信息安全事件：违反信息安全管理规定，性质较轻，没有造成公司损失。

一级违规：违反一级行为规范，或造成一级、二级信息安全事件。

二级违规：违反二级行为规范。

三级违规：违反三级行为规范，或造成三级信息安全事件。

四级违规：违反四级行为规范，或造成四级信息安全事件。

绝密信息资产：包括决策类（公司尚未公布的发展战略、经营策略；公司高管行程、与外部机构来往情况及其载体；公司董事长会议资料、纪要、会议内容等；公司重要的决策、变革、管理体系等；各级注明密级的文件、简报等资料及其载体）、销售类（未发货的意向客户清单；未发货的销售意向、合同与订单；首次开机前的发货单；批量的客户信息、销售意向、销售订单、发货单、GPS 监控数据）、研发类（研发计划、可行性分析报告及其评审纪要、总体目标、总体设计方案、研发项目任务书、产品工艺文件、成套产品设计图纸、关键零部件设计图纸），财务类（物料成本、应收货款、利润表、现金流表、资产负债表等），对公司利益或品牌形象可能造成重大负面影响的信息，由 CRM、SCM 定义的绝密资产，以及由各业务部门认可的绝密信息资产。

各部门归口 IT 负责部门：以组织架构为基础，按员工终端或办公实际所在地点，如在本一级部门组织架构内，所在地无 IT 支持人员的，则由当地 IT 支持部门负责，否则由本一级部门组织架构内 IT 部门负责。

4 职责

员工：员工应对所保管的信息资产的安全性负首要责任，并有义务遵循公司各类安全要求及安全策略。

员工直接领导：对员工的信息安全意识宣贯工作负首要责任；三级以上信息安全事件发生后，负连带责任。

员工所在一级部门负责人：部门信息资产的总体负责人，部门绝密资产定义的最终审批人，本部门信息资产对外交流许可的最终审批人。

各部门归口 IT 负责部门：保证提供给员工的初始 IT 工具、环境等符合信息安全要求，并定期对其进行检查。

5 行为规范

5.1 一级行为规范

严禁在公司内或针对公司进行黑客攻击、监听数据、端口扫描、窃取密码、嗅探网络等非法操作。

严禁在公司内编写、搜集、传播病毒木马与黑客软件。

严禁攻击公司网络和信息系统。

严禁窃取、盗卖公司保密信息。

严禁绕过公司安全控制系统。

严禁未经批准，通过拍照、摄像、录音等方式获取公司的保密信息。

严禁窃取他人帐户盗取保密信息、篡改系统数据等。

严禁在信息安全违规事件调查过程中，存在销毁证据等行为。

严禁散布公司大量绝密资料。

严禁故意散布对公司利益或品牌形象可能造成重大负面影响的信息。

5.2 二级行为规范

禁止私自修改办公电脑安全策略配置。

禁止在未经许可的情况下，将所持有的公司设备、信息、软件带出公司或挪做工作以外的他用。

禁止在个人私自在公司内部搭建有线、无线网络或提供互联网(WEB)\文件服务器(FTP)\代理(Proxy)\动态地址（DHCP）\邮件服务器（SMTP\POP3）等服务。

禁止将未启用公司安全准入软件与准入策略的自带计算机、手机、平板等设备接入公司网络、系统。

禁止在连接到三一内部网络的同时，用电话拨号、无线或其它方法连接到非三一网络。

禁止通过 OA 传送、邮件发送研发图纸文件。

禁止未经审批流传公司绝密资料。

禁止私自处理损坏的个人计算机，仅可由 IT 服务人员进行硬件检测和拆卸等工作。送厂商维修前，必须由 IT 服务人员将硬盘拆除交至 IT 资产管理员；如个人终端遇到硬盘损坏故障，损坏硬盘必须交予 IT 资产管理员进行消磁处理后方可退回厂商。

禁止私自携带硬盘出门进行维修，硬盘出门维修必须走 OA 流程申请，流程见 IT 类/IT 设备管理/其它类/硬盘出门维护申请。

集团早会等绝密、保密会议，禁止携带手机、录音设备、摄像设备入内，详见《三一重工会议安全管理制度》。

禁止未经批准，删除 IT 系统的日志。

禁止系统管理员私自查看、创建、修改、删除关键业务数据或授予无关人员系统权限。

禁止未经授权，系统管理人员对系统所承载的业务数据进行创建、修改、删除、查看、收集、下载打印、传播等。

禁止隐藏、伪造个人身份使用公司信息系统，如假冒他人邮件帐户发送邮件。

禁止保存或散布对公司利益或品牌可能造成较大负面影响的信息。

5.3 三级行为规范

非机要区域工作人员不得擅自进入机房、档案室、研发区及其它机要区域；不得擅自带领无关人员进入机房、档案室、研发区及其它机要区域；进入该类区域应按照此区域安全访问要求执行。(如《泵送信息安全管理规定》要求在某些重点管控区域不得携带智能手机等)

禁止携带私人笔记本电脑进入研发区域。

禁止未经审批流传公司涉密资料。

禁止将笔记本电脑接入研发网络；如需要在研发区域内使用笔记本电脑，必须封堵笔记本电脑网口。

禁止私自卸载办公电脑上预装的安全软件，包括杀毒软件、Inode 等。

内部发送密级资料需加密，密码不许随同文档发送。

在公司办公区域，禁止使用办公电脑擅自连接到非三一网络，禁止连接未经许可的无线设备。

外发邮件需抄送部门主管（部助级或以上级别），部门领导对外发邮件的安全性负连带责任，禁止以“回家加班”等私人需求相关的理由将工作邮件发往外网邮箱。

禁止私自撬开电脑机箱封胶或打开计算机机箱，发现接口封胶脱落以及资产标签脱落情况，需立刻上报 IT 部处理。

公司资料传送给他人时，应按需提供，只传递接收者职责范围内的内容，对于各单位的汇总信息，应加以区分，分别传送，禁止将统计信息，不做区分，直接群发各单位。

禁止收集、存放非本岗位的公司密级数据，禁止在未经授权的情况下打印受控资料。

禁止使用私人手机、相机、录音设备等设备对公司电脑屏幕、文件资料、会议、对话等进行记录。

禁止使用他人的账号、IP，不得将个人账号、IP 借给他人使用。

禁止在多台计算机上使用同一账号登陆 PDM 系统。

禁止在任何接入公司内网的终端上安装远程控制类软件，windows 系统自带的远程桌面功能除外。

通过 USB 拷贝资料必须通过审批，流程见集团固化流程/IT 类/公共应用权限/USB 拷出申请。

禁止未经批准，系统管理人员私自改变生产环境中设施、设备、系统的用途。

禁止保存或散布对公司利益或品牌可能造成负面影响的信息。

5.4 四级行为规范

在所有系统中设置的系统口令长度至少大于 8，且必须为数字、字母、特殊字符无任何规律组合。

员工离开办公位时，必须立即锁定计算机屏幕；离开电脑 3 小时以上时，应关闭电脑主机，特殊情况除外（如系统测试、数据收集等）。

接口部门和负责人，需对接待的第三方人员在司行为进行监督，一旦发现第三方访问引起的信息安全异常和安全事件时，员工应立即通知信息系统所属部门和信息安全部门，关闭其所有权限，并配合调查。

员工离司前，直接主管应负责考察其所拥有的系统权限关闭情况和信息资产移交情况。

不得使用公司的系统散布、转发或回复连锁邮件、恶作剧邮件及其他一些与业务无关的邮件。

不得设置匿名完全共享文件夹。

不得利用公司资源访问不健康网站；不得利用公司资源处理私人事情；不得在工作时间访问与工作无关的网站、玩游戏等。

未经授权不得安装非标准软件。

员工使用打印机打印文档时，打印完成后立即从打印机上取回文档；如遇打印机故障，应立即取消设置的打印任务，防止信息泄露。

未经审批，不得私自在办公电脑上新建或使用本地账号，发现存在启用的本地账号，需立刻上报 IT。

因工作，需暂时打开远程桌面的，时长不得连续超过 12 小时。

在无人值守情况下，将涉密文件放在会议室、复印和传真室等场所。

涉密文件应放置在安全场所，离开座位前，应清空办公桌上摆放的涉密信息文件；应随时锁上抽屉与文件柜，并将钥匙存放在安全的地方。

员工应定期自查计算机物理加封状况，如发现封条脱落等情况，应及时报告给信息安全责任部门，并联系 IT 人员或帮助台进行相应整改。

当发生信息安全异常，员工需立即向各级领导以及 IT 部门、600 帮助台报告，报告内容应包括他们观察到或怀疑的任何系统或服务的安全弱点,必要时提供事件分析过程报告。在进行信息安全事件的调查时，员工应积极配合。

6 其他说明

6.1 所有员工必须按要求参加信息安全培训活动及考试，考试缺考或不及格的人员，发生信息安全事件的，对其处罚将上升一级。

6.2 流程审批人需对其审批的内容负起安全责任，如因此发生信息安全事件，需负连带责任。

6.3 邮件外发及 USB 拷贝文件的相关要求详见《信息监察管理制度》。

6.4 除以上规范外，因员工行为导致的信息安全事件，由违规处理部门（审计监察总部、信息安全科、PDM 管理部等）初定其事件等级，并经被处罚人或损失部门确定后决定。

7 奖惩措施

违规等级	处罚标准	连带责任处罚标准	举报奖励标准
四级	30 分及以下扣分；	连带处以 15 分及以下扣分；	50 至 200 元现金奖励
三级	第一次违规 30—100 分扣分； 第二次违规除以上处罚外，剥夺相应权限，半年内不得申请	连带处以 10-50 分扣分；	200 至 500 现金奖励
二级	第一次违规半年度绩效不得为“中上”及以上； 第二次违规年度绩效不得为“中上”及以上，剥夺相应权限，半年内不得申请	连带处以 20-100 分扣分；	
一级	开除	半年度绩效不得为“中上”及以上	500 至 10000 元现金奖励

8 相关文件

8.1 《行政处罚管理制度》

8.2 《信息安全审计管理制度》

8.3 《信息监察管理制度》

8.4 《第三方人员信息安全管理规定》

8.5 《泵送信息安全管理规定》

8.6 《三一重工会议安全管理制度》

9 附件

无

10 附加说明

本制度由流程信息化总部系统运维部信息安全科起草，并负责解释和归口管理。