涉密保密系统的三员管理 贯标集团 保密三员是哪三员？

产品名称	涉密保密系统的三员管理 贯标集团 保密三员是哪三员？
公司名称	贯标集团
价格	.00/件
规格参数	
公司地址	南京市仙林大道10号三宝科技园1号楼B座6层
联系电话	4009992068 13382035157

产品详情

保密法第二十三条规定，存储、处理国家秘密的计算机信息系统〔以下简称涉密信息系统)按照涉密程度实行分级保护。

根据分级保护有关规定和国家保密标准要求，涉密信息系统应当配备系统管理员、安全保密管理员和安全审计员三类安全保密管理人员(简称为“ 三员 ”)，分别负责系统运行、安全保密管理和安全审计工作。

“ 三员 ”担负维护系统安全、稳定、可靠运行的重要任务，对涉密信息系统和国家秘密安全具有重要作用。

设立“ 三员 ”的必要性

“ 三员 ”是相对于超级管理员而提出的概念，旨在划分涉密信息系统管理权限，确保对系统的管理行为受到限制和监督。

一般来说,超级管理员对系统具有不受限制的完全访问权限,能够新建、删除各种用户和管理员账号，对硬盘文件进行各种操作，随意安装软件程序，任意修改系统和网络设置。

一旦超级管理员发生违规访问和操作，系统就没有任何安全可言。因此，涉密信息系统必须删除超级管理员账号，将系统管理划分为“ 配置、授权、审计 ”三种相互独立、相互制约的权限，由系统管理员、安全保密管理员、安全审计员分别掌握。

以系统新增用户为例，比如，经批准系统将新增一个用户名为“ user ”的用户，可以访问机密级以下信息,具体操作是:系统管理员新建账号“ user ”:安全保密管理员为“ user ”账号授予机密级以下信息访问权限:安全审计员查看系统中系统管理员和安全保密管理员增加“ user ”账号并授权的操作记录，对照工作审批单进行审计,以确定系统管理员、安全保密管理员的操作是经过授权和批准的。这样，对系统的一项配置须由两个管理角色配合才能生效，第三个管理角色进行监督和审计，避免了因管理权限过大而带来的安全保密风险。

涉密信息系统中的网络设备、安全保密设备、服务器和用户终端、操作系统、数据库、涉密业务应用系统的管理原则上都应由系统管理员和安全保密管理员配合完成，由安全审计员进行审计。在实际管理过程中，如果从技术上可实现某项配置两人操作方可生效，则将该项配置分工于系统管理员和安全保密管理员来完成，并由安全审计员对操作日志进行审计。

如果从技术上不能实现配置操作的分工，例如，交换机、路由器等通用网络设备本身没有划分“ 三员 ”功能，但能记录操作日志，则要求由系统管理员或安全保密管理员完成相关操作后，由安全审计员对操作日志进行审计。

“ 三员 ”的主要职责

“ 三员 ”并不是特指三个人，而是代表涉密信息系统安全保密管理的三类岗位或角色,对应不同的职责,由相关人员担任，以相应权限的管理员账号登录设备或系统来完成各项工作。

具体分工是:系统管理员主要负责系统的日常运行维护，包括网络设备、安全保密产品、服务器和用户终端、操作系统、数据库、涉密业务应用系统的安装、配置、升级、维护、运行管理;网络和系统的用户增加或删除;网络和系统的数据备份、运行日志审查和运行情况监控;应急条件下的安全恢复，等等。

安全保密管理员主要负责系统日常安全保密管理,包括网络和系统用户权限的授予与撤销:用户操作行为的安全审计;安全保密设备管理:系统安全事件的审计、分析、处理;应急条件下的安全恢复，等等。安全审计员主要负责对系统管理员、安全保密管理员的操作行为进行审计分析和监督检查，以及时发现违规行为。

此外，“ 三员 ”还应承担保密和信息化部门赋予的其他相关工作。比如,管理设备台账，组织设备维修,定期对涉密信息系统使用人员进行培训，配合开展涉密信息系统安全保密测评审批、保密检查等工作。

“ 三员 ”的配置

根据中央有关文件规定，涉密信息系统“ 三员 ”应当由本单位内部人员担任。担任涉密信息系统“ 三员 ”的人员，政治上应当可靠，应熟悉涉密信息系统管理操作流程,具有较强的责任意识和风险防控意识。

、

在实际工作中，网络设备、安全保密设备、服务器、用户终端、操作系统、数据库等通用设备和系统的管理,技术性要求较高,管理这些设备和系统的系统管理员、安全保密管理员可由信息化部门专业技术人员

担任。

对于涉密信息系统中运行的一些业务性比较强的涉密应用系统,如人事管理系统、财务管理系统等，对业务要求相对较高，因此,管理这些业务应用系统的系统管理员、安全保密管理员可由相关业务部门的人员担任。

此外，各类设备和系统的安全审计员可根据工作需要，由保密部门或其他能够胜任安全审计员工作的人员担任。需要注意的是，同一设备或系统的系统管理员和安全审计员不得由同一人兼任,安全保密管理员和安全审计员也不得由同一人兼任

“ 三员 ”的培训

我国实行涉密信息系统“ 三员 ”持证上岗制度。中央有关文件规定,系统管理员、安全保密管理员和安全审计员应当经过保密行政管理部门组织的培训,持证上岗。

“ 三员 ”只有接受专业知识培训并通过资格考试,取得国家保密行政管理部门统一颁发的资格证书后，才能上岗履行职责。

在实际工作中，由于网络设备、安全保密设备、服务器、用户终端、操作系统、数据库品牌和型号的不同、业务应用系统的不同,安全保密管理策略配置和操作会存在差别。

因此，“ 三员 ”在参加培训的基础上，还应认真研究掌握所管理的具体设备或系统的配置和操作，将涉密信息系统分级保护技术标准和管理规范各项要求落到实处。

“ 三员 ”的监督

“ 三员 ”应在本单位保密和信恳化部门的监督下开展工作，确保所有的操作都是符合规定或经过授权的。可以从三个层面对“ 三员 ”工作进行监督。

一是内部监督。机关、单位的保密和信息化部门定期对“ 三员 ”工作情况进行检查和考核,对“ 三员 ”未能按规定履职的情况及时予以纠正。

二是上级监督。主要针对机关、单位跨部门或者跨地区的涉密信息系统，机关、单位应定期对其远程网络或远程终端的“ 三员 ”工作情况进行检查和考核,对“ 三员 ”未能按规定履职的情况，及时通知远程网络或远程终端使用单位予以纠正。

三是保密行政管理部门监督。“ 三员 ”工作情况是保密行政管理部门依法开展网络保密检查的重要内容，在履行保密检查职能的过程中，保密行政管理部门也应定期对“ 三员 ”履职的情况进行检查。