

基于信息安全的军工企业信息设备全生命周期管控与实现

刘嘉怡

(成都飞机工业(集团)有限责任公司, 四川, 成都, 610092)

摘要: 信息设备是企业运行的主要物质技术基础之一, 能大幅提高企业信息管理的效率和水平, 然而军工企业的信息设备不仅关系到企业的生产运营, 还关系到国家信息的安全保密, 所以军工企业信息设备管理的重要性和特殊性毋庸置疑。本文基于国家安全保密新标准, 探讨信息设备全生命周期的流程化管理问题。

关键词: 信息设备; 信息孤岛; 流程; 信息安全; 管理

Abstract: The information equipment is one of the main material basis for enterprise operation, which can greatly improve the efficiency and the level of information management of enterprises. However, information equipment in military enterprises is not only related to the production and operation of the company but also to the national information security, so there is undoubtedly the importance and particularity of information equipment management of military enterprises. Based on the new standard of national security, this paper describes the management of life-cycle information equipment.

Key words: Information Equipment, Information Silo, Process, Information Security, Management

0 引言

传统的设备管理关注设备的综合效率, 对设备的质量运动和价值运动进行全过程(规划、设计、选型、购置、安装、验收、使用、保养、维修、改造、更新和报废)的科学型管理, 而军工企业的信息设备管理在传统设备管理的基础上, 在可靠性、保密性、系统灾难恢复、数据存储安全和访问控制等方面都有着严格的要求, 且信息设备全生命周期管理各个流程环节产生的资料又成为确保安全保密的重要依据, 对提高信息安全服务效能和决策分析有着重要作用, 信息安全保密的保证又为军工企业的运营提供可靠的保障, 军工企业的信息设备管理, 是基于信息安全的设备管理。

1 新形势下各业务领域对信息设备管理提出新要求

传统的信息设备管理系统主要面向日常业务及数据处理, 无法为军工企业的管理决策提供多视角、多维度的信息支持。设备管理、财务管理、经营管理、信息安全管理、运维管理和质量管理, 以及业务流程的整合及融入, 对于军工企业的信息设备管理至关重要。通过流程设计把信息设备全生命周期产生的各业务领域的管理起来, 并使之贯穿多应用系统、数据和用户, 优化管理环节, 明确管理职责, 强化过程监控, 从而为“数字军工”建设和发展提供有效的安全保障。

2 国家安全保密对信息设备管理的要求

《武器装备科研生产单位保密资格标准》规定：应当建立信息设备和存储介质台账。单位应当通过监理信息设备总台账，加强计算机和信息系统的资产管理。总台账应包括本单位的各类信息设备，通常有计算机、网络设备和外部设备、存储介质、安全保密产品等。单位各部门应当监理相应的分台账，总台账和分台账的内容应相互吻合。单位应制订严格的设备与介质全生命周期管理制度，建立设备采购、携带、维修、变更和报废审批流程^[1]。

3 传统信息设备管理存在的问题

传统的基于职能的信息设备管理模式强调阶段的划分及有序性，各业务部门的工作目标、范围及关注重点不同，各部门更关注各自领域的优化，缺乏沟通协调，欠缺对信息设备的全生命周期的过程管理，具体表现在以下几个方面。

(1) 采购信息设备缺乏可靠的参考依据，选型盲目，无前瞻性和计划性，无历史数据参考，在信息设备选型时只考虑满足当前需要，不考虑后期运维和耗材成本，造成后期运维成本居高不下。

(2) 各职能部门及使用单位按照各自业务需求建立台账，造成“账、卡、物”不一致。

(3) 信息设备全生命周期管理流程繁琐，涉及设备管理、财务管理、信息安全管理、运维管理和质量管理等内容，各业务流程环节之间的衔接缺乏主导，出了问题查源头困难。

(4) 无专门的信息设备管理软件，管理难度大。如信息设备变更、迁移、报修、维修后需手工变更台帐，造成台帐信息不清晰和变更滞后等现象。又如，报表生成困难，相关部门无法及时获取信息设备台帐信息。

(5) 管理体制不健全，责任不明确，设备管理部门、财务部门、信息安全管理部门、运维部门和使用单位形成一种谁都能管，谁都管不了的局面，使用人员只管使用，不管不顾安全、运维和质量对信息设备的管理要求。

4 建立全新信息设备管理体系架构和信息设备管理人员组织，明确业务分工

4.1 设备管理网络

建立四级信息设备管理网络，确保各领域管理措施落实到位，依照“谁使用，谁负责；谁主管，谁指导”的原则，

确立设备责任人、部门系统管理员、公司信息设备管理员（原资产管理人）和各业务领域管理员。如图 1 所示。

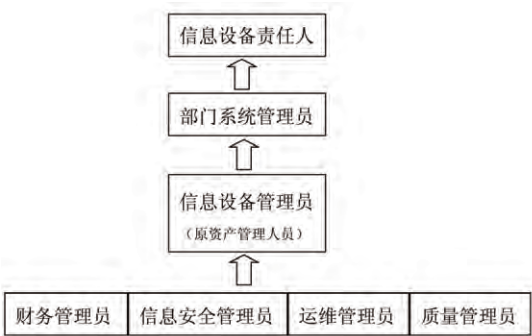


图 1

4.2 信息设备管理人员

基于军工企业的信息设备管理的特殊性，人员配置应适应设备管理、财务管理、信息安全管理、运维管理、质量管理和客户管理的需要，熟悉各业务模块对信息设备管理的基本要求。传统的基于财务管理及库房管理的信息设备管理方式会导致信息设备服务体系成为“信息孤岛”，设备管理、财务管理、信息安全管理、运维管理和质量管理不断研究各自关注的信息设备管理方式，建立各自的信息设备管理要求，可能导致管理要求相互脱节不兼容。

4.3 人人参与信息设备管理

强化现场管理，每个岗位和每位职工都参与信息设备管理活动，确保自己使用的信息设备不因无知而泄露，部门系统管理员宣传、巡检、监管及时发现问题，各业务领域提出各自关注的信息设备管理要求，公司信息设备管理人员，制订具体的信息设备管理制度。做到层层把关、人人参与，这样的军工企业信息设备管理才不会有真空状态。

5 建立信息设备管理系统，实现流程化管理

5.1 建立完善的管理系统

完善的系统建设能够实现对于信息设备全生命周期的有效管理，通过对各个流程环节监督的设立，做到实时监控每个过程，形成完整的信息设备基础数据及档案，满足对各种设备、各种属性、各种状态、各个流程节点的管理及监控要求。流程环节生成的各种数据及表单为信息设备的安全保密管理、财务管理和经营管理提供便利，在建立完善的信息设备管理库基础上，形成信息设备资源库。

5.2 信息设备管理的三个阶段

一是信息设备前期管理阶段，主要包括信息设备的规划、评估、选型、采购和验收等；二是信息设备中期管理阶段，即设备运行使用管理阶段，主要包括入库、验机、申请、分配、运维和维修等，该阶段是信息设备为企业创造价值的时期；三是信息设备后期管理阶段，主要是信息设备报废及存储介质的销毁管理，此阶段重点需要关注的是涉密载体的拆除、交接及消磁、销毁问题。信息安全关注的主要是第二阶段和第三阶段的信息设备管理，以信息安全为理念基础，搭建信息设备管理生命周期管理的框架如图 2 所示。

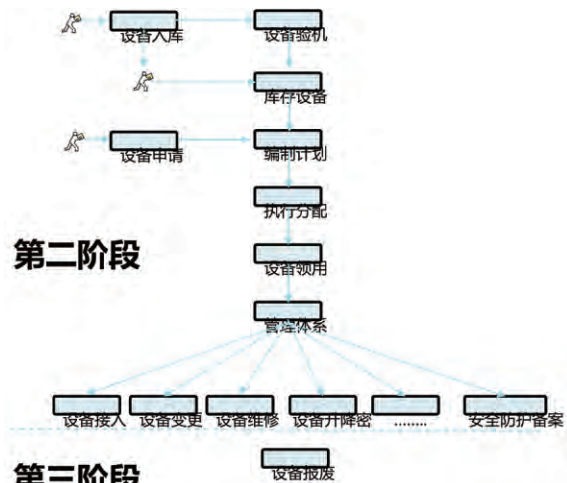


图 2

5.3 系统功能模块设计及描述

本系统从以下功能模块进行流程设计：“系统管理”、

“设备入库管理”、“计划管理”、“配件管理”、“设备台账管理”、“设备流程管理”、“专用设备管理”、“IP 地址池管理”、“软件资产管理”和“报表管理”，系统总体框架如图 3 所示。

5.3.1 信息设备入库管理

信息设备到货后，有信息设备管理员（原资产管理）核对合同与实物一致后，在系统中登记入库，入库后在系统中登记信息设备财务相关信息后进入验机环节，不需要验机的设备直接进入待分配环节。

5.3.2 信息设备验机管理

由信息设备技术管理部门对已入库的需要验机的信息设备的配置信息进行检查登记。如计算机需要登记的主要信息有计算机硬盘、网卡、内存、CPU、显卡和显示器。

5.3.3 信息设备分配管理

由部门系统管理员发起信息设备使用申请，经申请单位主管领导审批通过后，由信息设备分配人员根据申请单及当前申请信息设备的库存状态编制分配计划，再由信息设备管理员根据分配计划分配对应型号的信息设备，分配完成后，由申请单位部门系统管理员领取设备。

5.3.4 信息设备配件管理

信息设备在维修、硬件升级、信息设备密级变化、不再使用时办理退库手续，不同部门之间的资产调拨均可能使用到信息设备配件，什么原因使用，如何使用，用在哪台设备上，均需要通过流程进行监控关联。特别是硬盘的管理，由于处于涉密信息系统大环境下，所以其所有的使用及变化



图 3

都应纳入监控范围。

5.3.5 信息设备台账管理

信息设备纳入统一管理后,需要一个入口对数据信息进行查看。层层把关、人人参与的具体实施方式就是通过信息设备台账检查实物的实际情况。信息设备责任人通过“个人台账查看”检查自己名下的信息设备信息是否与实际情况一致;部门系统管理员抽查、监管及时发现问题;各业务领域根据信息设备总台账查看自己业务领域关注的信息。

5.3.6 信息设备流程管理

因军工企业涉密信息系统安全保密要求的特殊性,信息设备安全作为物理安全的重要部分,所有的信息设备属性的变化都需要流程进行监控,通过流程驱动变化,是军工企业信息设备管理的基本要求,任何变化都不能通过人工进行修改,任何变化都需要有审批有依据可查询。

可能的流程有:信息设备接入(入网)流程、信息设备变更流程、信息设备维修流程、信息设备密级变更流程(因为军工企业信息设备密级的变化是极为重要的数据,所以单独设计流程进行监控)、信息设备停用流程、信息设备启用流程、信息设备报废流程、信息设备借用流程和信息设备备案流程。

5.3.6.1 信息设备接入(入网)流程

由部门系统管理员发起本单位的信息设备接入流程。通常军工企业的网络为局域网,所以接入流程分为接入军工局域网、互联网和单位某些应用建立的局域网。系统根据不同类型的信息设备接入不同类型的网络,应做不同的流程流向控制。

5.3.6.2 信息设备变更流程

信息设备在由部门系统管理员领用后,交由信息设备责任人使用,使用过程中会产生较多的变化,由于军工企业的特殊性,信息设备的所有变化过程及结果都是档案资料,故信息设备的任何变化都需要审核和记录,才能形成完整的信息设备基础数据库及档案。

通常信息设备在领用后,用户在使用过程中可能会变更的内容有:基本属性变更,如硬盘信息(因验机录入时手工录入错误)、光驱信息(只读、刻录、无光驱)、网卡信息(因验机录入时手工录入MAC地址错误)、操作系统安装时间等;管理属性变更,如责任人、使用人、安装位置、用途和密级等;配置属性变更,如需要增加网卡、增加硬盘、

增加内存或光驱等。

5.3.6.3 信息设备维修流程

由部门系统管理员负责发起本单位信息设备维修流程。由本单位主管领导审批同意后,经信息设备维修部门检查,根据信息设备的实际损坏程度综合维修部门的技术能力,决定信息设备是内修还是外修,内修由信息设备维修部门实施维修。由于军工单位的特殊性,外修由信息设备维修部门人员对维修设备做安全处理后,全程陪同外修。最终将维修结果告知信息设备责任单位部门系统管理员。

5.3.6.4 信息设备退库流程

人员离职或其他原因造成计算机等设备长期闲置,可以发起设备退库流程,由信息设备管理人员进行再次分配。因军工企业信息设备的特殊性,避免扩大涉密信息的知悉范围,具备存储功能的信息设备,如计算机、服务器需由信息设备主管单位对计算机设备进行更换硬盘后方能再次分配。

5.3.6.5 信息设备升降密流程

军工企业的信息设备密级与人员密级有密切的关联关系,由于信息设备使用人的密级或信息设备用途发生变化时,信息设备的密级都需要发生相应的变化,由部门系统管理员发起信息设备升降密流程。由信息设备主管单位对信息设备进行相应处理,或重新安装操作系统或者更换硬盘。

5.3.6.6 信息设备停用

由于军工企业的特殊性,信息设备责任人如因工作原因临时借调、出差导致短期内不会使用信息设备时,由信息设备责任单位的部门系统管理员发起信息设备停用流程,经信息设备主管单位审批后,信息设备的台账状态更改为“停用”。如果是计算机设备停用,还需要做网络端口处理,禁止设备访问网络权限,以防止违规接入设备对系统资源的访问。处于“停用”状态的计算机设备,不需要及时更新计算机病毒库及升级系统补丁。

5.3.6.7 信息设备启用流程

停用设备需要重新启用时,由设备使用单位部门系统管理员发起信息设备启用流程,如果是联网的信息设备,还需经信息设备主管单位开启信息设备访问网络权限,再将信息设备状态更改为“使用中”。

5.3.6.8 信息设备设备报废流程

由于信息设备达到使用年限或因故障已无法修复,由使用单位部门系统管理员发起信息设备报废流程,经信息设

备主管单位进行安全处理后,将信息设备进行物理报废处理。具有存储功能的设备需要拆除存储固件,能做消磁处理的需要消磁。

5.3.6.9 信息设备借用流程

由信息设备主管单位提供一些信息设备,以供企业中临时性工作需要使用,由于军工企业的特殊性,以供借用的信息设备需要严格按照安全保密要求进行管理。

企业各信息设备使用部门,由用户单位部门系统管理员提起信息设备借用申请,报信息设备主管部门处理后,通知借用单位部门系统管理员领取设备,用户单位使用后,由借用单位部门系统管理员负责归还到信息设备管理部门,进行信息安全检查后再返回入库。

5.3.6.10 计算机安全保密防护备案、消除流程

军工企业信息设备因安全保密要求,要安装防病毒、审计软件,纳入域管理、回收管理员权限设置用户、开放端口需审批等,这部分信息同样也是信息设备管理的重要部分,是否按要求进行安装、部署,未安装是否按要求进行备案,纳入信息设备管理系统管理后,与信息设备关联,更利于管理。

5.3.7 信息设备运行状态流程查询描述

信息设备在运行过程中的所有变化及产生的数据都是确保安全保密的重要依据,对提高信息安全服务效能和决策分析有着重要作用。本模块主要对设备接入、变更、维修、停用、启用、升降密、借用、报废和计算机设备备案/消除流程进行查询。

5.3.8 信息设备台账查询

本功能模块查询所有的信息设备台账信息,查询登陆者所在部门的所有信息设备台账信息,查询资产归口为本部门的信息设备台账信息,查询登陆者为责任人的信息设备信息。

5.3.9 软件资产管理

管理企业软件资产信息,并对软件资产的 License 分类、分模块管理,并提供 License 到期提醒。

5.3.10 IP 地址池管理

加强信息设备接入管理,控制违规接入设备对系统资源的访问,管理企业信息设备需要配置的网络资源是首要工作。按责任部门、IP 使用范围、IP 密级、信息设备所在楼宇和设备密级等物理属性分类管理 IP。信息设备的 IP 地址与 MAC 地址绑定。信息设备安装位置变化,维修更换了网

卡或者主板(网卡集成)、密级发生变化或信息设备报废,都可能涉及 IP 地址的重新分配,将 IP 的分配、回收纳入 IP 地址池管理,随时监控网络资源的使用情况。

6 完善信息设备管理各项制度

完善的信息设备管理,除了建立信息设备管理系统设置流程化管理外,还需要制定全面的信息设备全生命周期管理制度,使设备管理人员、使用人员有规可循、有章可守、有疑可查。

信息设备前期管理阶段,需要建立选型与采购安全管理相关制度;信息设备中期管理阶段,应建立信息设备资产管理制度、信息设备标识与编号管理制度、借用信息设备管理制度、信息设备台账管理制度、信息设备使用及运维管理制度、信息设备维修管理制度、信息设备配件管理相关制度、信息设备使用客户管理相关制度及要求、信息交换管理制度;信息设备后期管理阶段,主要是信息设备报废及存储介质的销毁管理,此阶段应建立信息设备报废管理相关制度,明确报废流程及报废过程中需要注意的安全保密事项。

7 信息设备管理系统在军工企业管理运用的前景

军工企业的信息设备管理系统的成功运行是基于基础数据的流程化管理,数据的准确性、及时性和可靠性是以信息设备全生命周期各业务流程环节的全面性、完整性和准确性为基础的,规范信息设备管理是军工企业实现两化融合及确保国家秘密不被泄露的重要手段。

规范的信息设备管理能最终实现对安全保密、运维管理,设备管理、客户关系管理及供应链管理等各个环节的科学管理,实现数据共享,建立信息资源库,统筹信息资源建设。IM

参考文献

- [1] 国家国防科技工业局,军工保密资格审查认证中心.《军工涉密信息系统安全保密管理人员工作实务》[M].北京:北京航空航天大学出版社,2011: 85-89