中华人民共和国国家军用标准

军队通用计算机系统使用安全要求 GJB 1295—91

Operation security requirements for military general—purpose computer system

1 范围

1.1 主题内容

本标准规定了军队通用计算机系统在使用中的实体(场地、设备、人身、媒体)的安全管理与技术要求;预防病毒及防止信息泄漏的措施;安全审计、安全风险分析的内容、应急计划的制定等。

1.2 适用范围

本标准适用于军队各类通用计算机系统。其它计算机系统亦可参照执行。

2 引用文件

GB 2887—82 计算站场地技术要求
GB 4943—85 数据处理设备的安全
GB 9361—88 计算站场地安全要求
GJB 151—86 军用设备和分系统电磁发射和敏感度要求
GJB 152—86 军用设备和分系统电磁发射和敏感度测量
GJB 322—87 军用小型数字电子计算机通用技术条件
GJB 900—90 系统安全性通用大纲
GJB 511—88 军用微型计算机通用技术条件

3 定义

3.1 计算机系统 computer system

按人的要求收集和存储信息,自动进行数据处理和计算,并输出结果信息的一台或多台计算机组成的系统。它由硬件系统和软件系统两部分组成。

3.2 计算机机房 computer room

计算机系统及有关附属设备的安装使用场所。

3.3 风险分析 risk analysis

鉴别风险及确定其可能达到的限度,判定潜在的损失,并为制定保护策略提供依据的过程。

3.4 特定终端设备 specific—terminal unit

国防科学技术工业委员会 1991—12—23 发布 1992—09—01 实施

用于系统管理或对重要数据存取处理的终端。

4 一般要求

4.1 军队通用计算机系统的场地及设备应符合 GB 2887、GB 4943、GB 9361 中的要求。

4.2 对所有媒体的保护和管理应按照本标准执行。

4.3 军队通用计算机系统应具备开通运行条件，并按照本标准进行管理，确保运行安全。

4.4 对计算机病毒的防治，应按照本标准及有关规定执行。

4.5 军队通用计算机系统设备应符合 GB 151、GB 152 的有关要求；对信息泄露发射应采取必要的防护措施。

4.6 对计算机安全风险分析应适时地组织专家进行，并根据风险分析结果，提出相应保护措施。

4.7 军队通用计算机系统应具备安全应急计划，并有相应的设备及软件备份。

4.8 计算机系统一般应有安全审计制度。安全要求高的计算机系统，必须具有安全审计制度，并按本标准执行。

5 详细要求

5.1 计算机场地及设备的安全技术要求

5.1.1 计算机机房的设计或改建应符合 GB 2887、GB 9361 和 GJB 322 等现行的国家标准。

5.1.2 除参照上述有关标准外，还应注意满足下述各条要求：

a. 机房主体结构应具有与其功能相适应的耐久性、抗震性和耐火等级。变形缝和伸缩缝不应穿过主机房；

b. 机房应设置相应的火灾报警和灭火系统；

c. 机房应设置疏散照明设备和安全出口标志；

d. 机房应采用专用的空调设备，若与其它系统共用时，应确保空调效果，采取防火隔离措施。长期连续运行的计算机系统应有备用空调。空调的制冷能力，要留有一定的余量(宜取 15%—20%)；

e. 计算机的专用空调设备应与计算机联控，保证做到开机前先送风，停机后再停风；

f. 机房应根据供电网的质量及计算机设备的要求，采用电源质量改善措施和隔离防护措施，如滤波、稳压、稳频及不间断电源系统等。

5.1.3 计算机系统中使用的设备应符合 GB 4943 中规定的要求，并是经过安全检查的合格产品。

5.2 媒体管理与安全要求

5.2.1 媒体分类

根据媒体上记录内容将媒体分为 A、B、C 三种基本类别。

5.2.1.1 A 类媒体：媒体上的记录内容对系统、设备功能来说是最重要的，不能替代的，毁坏后不能立即恢复的。

5.2.1.2 B 类媒体：媒体上的记录内容在不影响系统主要功能的前提下可以进行复制，但这

些数据记录复制过程较困难或价格较昂贵。

5.2.1.3 C类媒体：媒体上的记录内容在系统调试及应用过程中容易得到的。

5.2.2 媒体的保护要求

5.2.2.1 保留在机房内的媒体数量应是系统有效运行所需的最小数量。

5.2.2.2 A、B类媒体应放入防火，防水，防震，防潮、防腐蚀、防静电及防电磁场的保护设备中。C类媒体应放在密闭金属文件箱或柜中。

5.2.2.3 A，B类媒体应采取防复制及信息加密措施。

5.2.2.4 媒体的传递与外借应有审批手续、传递记录。传递过程中，媒体应放入金属箱内，必须采取必要的保安措施。

5.2.2.5 记录过重要信息的记录设备出现故障时，必须在军内或指定单位进行维修。不能维修，即行销毁。

5.2.2.6 重要数据的处理过程中，被批准使用数据人员以外的其它人员不应进入机房工作。处理结束后，应清除不能带走的本作业数据。应妥善处理打印结果，任何记有重要信息的废弃物在处理前应进行粉碎。

5.2.3 媒体的管理要求

5.2.3.1 媒体应造册登记，编制目录，集中分类管理，所有媒体的目录清单必须具有如下项目：媒体类别，信息类别，文件所有者，卷号，文件名及其描述，项目编号，适应日期，保留期限。

5.2.3.2 根据需要与存贮环境，记录要定期进行循环复制（半年至二年），并复制三份分处存放。

5.2.3.3 新的磁记录文件应有完整的归档记录。归档文件应清楚齐全，一旦投入运行，任何人不经批准不得进行增、删、改。

5.2.3.4 各种记录应定期复制到媒体上，送媒体库进行保管。

5.2.3.5 各种媒体不用时，应存入媒体库内。

5.2.3.6 未用过的媒体应定期检查，情况应例行登记。报废的媒体在进行销毁之前，应进行消磁或清除数据，并应确保销毁的执行。

5.2.3.7 媒体未经审批，不得随意外借。

5.2.4 建立媒体库

5.2.4.1 媒体库的选址应选在水、火等灾害影响不到的地方。

5.2.4.2 媒体库应设库管理员，负责库的管理工作，并核查媒体使用人员的身份与权限。

5.2.4.3 媒体库内所有媒体，应统一编目，集中分类管理。

5.3 计算机病毒的防治

5.3.1 计算机系统防病毒要求

5.3.1.1 应指定专人负责计算机病毒的防治工作。

5.3.1.2 加强终端管理，及时发现非法程序，并按有关规定及时清除。

5.3.1.3 计算机系统及其所用盘、带应定期检测、登录，一经发现病毒，立即禁止使用，并按有关规定进行病毒清除。

5.3.1.4 军用计算机在下列情况下，应指定专人对设备进行病毒检查，确认无病毒后方可投

入使用：

a. 从国外进口的计算机验机时；

b. 从国内市场自购或自行研制的计算机启用时；

c. 执行特殊任务前；

d. 计算机经外单位维修后；

e. 从外单位借入的计算机使用前。

5.3.2 媒体预防病毒的保护要求

5.3.2.1 重要部门媒体应做到专机、专用。

5.3.2.2 非本机使用的媒体，须经过检测，确认没有病毒，方可在系统中使用。

5.3.2.3 禁止执行不知来源的程序，禁止在计算机系统上运行任何游戏程序。

5.3.2.4 外借的媒体返回时，应进行病毒检查。

5.4 计算机系统电磁兼容性及防泄露发射要求

5.4.1 计算机系统所使用设备均应符合 GJB 151、GJB 152 标准的要求。

5.4.2 采用区域控制。

5.4.3 采用屏蔽措施。

5.4.4 采用低辐射设备。

5.4.5 采用其它安全防护措施。

5.5 计算机系统运行安全

5.5.1 安全管理

5.5.1.1 计算机系统运行管理部门必须设有安全组织或安全负 人。

5.5.1.2 安全组织或安全负责人职责如下：

a. 保障本部门计算机系统的安全运行；

b. 制定安全管理的方案和规章制度；

c. 定期检查安全规章制度的执行情况，提出改进措施；

d. 掌握系统运行的安全情况，收集安全记录，及时发现薄弱环节，研究和采取相应的对策，并及时予以改进；

e. 负责系统工作人员的安全教育和管理；

f. 向安全监督机关和上一级主管部门报告本系统的安全情况。

5.5.2 机房管理制度

5.5.2.1 建立规章制度：

a. 计算机系统维护管理制度，维护规定见 5.5.4 条；

b. 计算机管理的各种制度，参见附录 A(参考件)；

c. 计算机数据及文件的管理规章制度；

d. 计算机机房的管理制度，参见附录 B(参考件)；

e. 严格有效的出入管理规章制度，具体规定参照附录 C(参考件)；

f. 有关监视的管理规章制度，监视内容参见 5.5.5 条。

5.5.2.2 计算机工作人员责任

应规定计算机工作人员职责(内容包括:硬件值班人员职责、硬件维修人员条件、操作人员须知);计算机工作人员必须严格遵守有关规定和本系统的安全规章制度,维护本系统的安全。

5.5.3 运行及确认

5.5.3.1 所有交付使用的计算机系统应配有齐全的技术说明书。

5.5.3.2 计算机系统应备有操作说明书,操作人员必须严格执行操作规程。操作说明书内容见附录D(参考件)。

5.5.3.3 必须规定各种资源的使用权限,设置相应的存取控制及存取监视功能。

5.5.3.4 建立计算机系统运行记录,掌握每日运行情况。

5.5.3.5 制定计算机系统故障时的应急计划及应急措施。

5.5.3.6 系统管理员、程序员及操作人员应明确责任及分工。

5.5.3.7 大型计算机系统的操作应由多名专职操作人员执行。

5.5.3.8 对特定终端设备,应限定其操作人员,并采用口令、身份识别等措施。

5.5.4 计算机系统的维护

5.5.4.1 应制定计算机系统维护计划,确定维护检查的实施周期。

5.5.4.2 计算机系统的维护分为预防维护和故障维护。预防维护应定期进行,故障维护应及时分析原因找出问题,尽快恢复,并认真填写维护记录。

5.5.4.3 计算机系统各设备(包括主处理机、主存储器、磁盘机、磁带机、控打机等)应定期检查维护。

5.5.4.4 计算机系统维护时,对数据应采取妥善的保护措施。

5.5.4.5 计算机系统要定期进行故障统计分析。

5.5.4.6 必须建立计算机系统的维护档案。

5.5.5 机房的监视

5.5.5.1 计算机机房应视具体情况设置监视设备,及时发现异常状态,根据不同的使用目的可配备以下监视设备:

a. 红外线传感器;

b. 自动火灾报警器;

c. 漏水传感器;

d. 温湿度传感器;

e. 监视摄像机;

f. 其它。

5.5.5.2 安全人员应随时对机房进行巡视,注意发现产生危险、故障的征兆及其原因,检查防火防范设备的功能等。

5.5.6 人身安全及教育培训

5.5.6.1 计算机机房的布局应为工作人员创造一个良好的人机工作环境,确保长期工作人员的安全。

5.5.6.2 长期从事计算机工作的人员,应有劳保措施,并定期检查身体。

5.5.6.3 在使用说明书中应有操作、维护的安全注意事项。并在危险部位标以危险符号和警

告标记。

5.5.6.4 所有对地的电压(交流峰值或直流)大于 42.2V 的易触及部分,均应加以安全保护。

5.5.6.5 应定期对使用人员进行安全教育及培训。

5.6 安全风险分析

5.6.1 安全负责人应组织与系统有关的专家适时地对系统进行风险分析,风险分析的方法及结果应保密。

5.6.2 风险分析的内容:

a. 估算计算机系统及其有关设备、设施的价值;

b. 分析计算机系统的脆弱性,估算潜在的危险或可能引起的损失价值;

c. 估计发生风险的时间;

d. 分析现有的保护能力,制定相应的防护措施,并分析其安全效益。

5.6.3 风险可能造成的损失类型:

a. 计算机设备、设施的丢失、破坏和非授权使用;

b. 计算机软件与数据信息的破坏、丢失、非授权使用和修改;

c. 数据信息的失窃与泄露;

d. 其它损失。

5.7 应急计划及备份

5.7.1 计算机系统运行管理部门应根据下述可能出现的紧急情况制定相应的应急计划:

a. 计算机系统发生故障;

b. 误操作;

c. 外部攻击;

d. 发生火灾、水灾、地震等自然灾害;

e. 计算机病毒的侵蚀;

f. 意外停电;

g. 其它。

5.7.2 应急计划必须确定实施方案,制定紧急响应规程。

5.7.3 应定期对应急计划进行试验和修改。

5.7.4 将执行应急计划的有关文件放在规定的地方。

5.7.5 对执行应急计划的人员应进行培训,并实施演习,保证每个系统值班人员都能正确执行应急计划。

5.7.6 信息资源备份应按下列项目进行:

a. 全盘备份;

b. 增量备份;

c. 关键项目备份;

d. 后备媒体。

5.7.7 根据需要可采取下列设备备份方法:

a. 整机备份;

b. 关键部件现场备份；

c. 空调器、电源及辅助设备备份。

5.8 计算机安全审计

5.8.1 对安全要求较高的计算机系统，必须建立安全审计制度。

5.8.2 根据安全审计制度及本标准规定的安全要求，对计算机系统进行安全审计，审计结果应报上级机关。

5.8.3 按照审计要求改进安全控制后，审计人员应重新评价系统，以保证系统功能不退化。

附 录 A
计算机及计算机房管理的各种制度
（参考件）

A1 机时管理制度。
A2 计算机检修制度。
A3 仪器仪表管理制度。
A4 供电设备管理制度。
A5 配电室值班制度。
A6 空调值班制度。
A7 空调机维护制度。
A8 机房管理制度。
A9 机房技术管理。
A10 机房工艺卫生制度。

附 录 B
进出机房管理控制细则
（参考件）

B1 机房应采取分区控制。根据每个工作人员的实际工作需要，确定所能进入的区域。

B2 主机区共设一个受控制的出入口，另设若干备用口供紧急情况用。

B3 根据各区域的重要程度采取以下控制措施。

B3.1 挂“禁止入内”牌。

B3.2 派人看守，填写进出记录。

B3.3 关键入口可采用识别措施。

B3.4 进出口的钥匙，应保证在约定的场所，由专人管理，并制定严格的交接制度。

B3.5 机房无人时，应关锁进出口。

B4 对长期在机房工作的人员应定期发行带有照片的身份证及识别标志（徽章，明片）作为进出机房的识别。

B5 短期工作人员的进出，应持有临时出入证，并履行严格的登记手续。

B6 办事人员和来访者必须经有关领导批准后，由工作人员带领才能允许进入机房。

B7 携带物品进出机房时，应持有携物证。对可疑人员应检查其携带物品的内容，并在得到主管部门领导同意后，方可带入和带出机房。

B8 危险品及可燃品不得带入机房，用于维护设备或施工使用的物品，应妥当保管处置。

B9 未经有关领导批准，不得在机房内照像、录像。

附 录 C
计算机系统操作说明书内容
（参考件）

C1 系统操作顺序说明书内容。

C1.1 系统的操作方法。

C1.2 操作指令的使用方法。

C1.3 标准运行程序。

C1.4 有关其它系统的操作方法。

C2 系统操作说明整体联接系统图。

C2.1 整体联接系统图。

C2.2 各构成设备的详细安装图。

C2.3 各机器的工作原理简介。

C2.4 各部开关等操作部位的说明。

C2.5 各机器开关类的正常运行时的设定位置。

C2.6 异常状态的发现方法及操作说明。

C2.7 异常时的紧急联络点。

C2.8 设备的管理和操作及其它所必需的事项。

附加说明：

本标准由总参通信部提出。

本标准由总参第六十一研究所归口。

本标准由总参第六十一研究所负责起草。

本标准主要起草人：胡鹏、汪红宇、杨俊兰、李熙玉、刘凤昌、林杰璜、丁淀原、张杰、崔书昆。