QJ

中华人民共和国航空航天工业部航天工业标准

QJ 2560-93

航天办公信息系统计算机网络安全保密规则

1993-03-30 发布　　1993-10-01 实施

中华人民共和国航空航天工业部　发布

中华人民共和国航空航天工业部航天工业标准

QJ 2560-93

航天办公信息系统计算机网络安全保密规则

1 主题内容与适用范围

本标准规定了航天办公信息系统（以下简称航天 OIS）计算机网络的信息和数据的保密等级、机房及设备安全、传输安全、终端安全、存储安全、软件安全、人员管理及安全保密监督等方面的要求。

本标准适用于航天 OIS 计算机网络及有关的机构、人员。其它信息系统亦可参照执行。

2 引用标准

QJ 1236-87 信息系统数据安全与保密规范

QJ 1877-90 数据安全技术实施细则

3 术语

3.1 特定终端设备：可对重要数据进行存取的终端、有控制台功能的终端、系统管理员所用的终端。

3.2 实体安全：为保证计算机系统安全可靠运行，确保计算机系统在对信息进行采集、处理、传输、存储过程中，不致受到人为的（包括未经授权使用计算机资源）或自然因素的危害，而使信息丢失、泄漏或破坏，对计算机设备、设施（包括机房建筑、供电、空调等）、环境、人员等采取适当的安全措施。

4 保密等级

4.1 根据信息和数据的秘密性和重要性确定保密等级。

4.2 信息保密等级分为五级：绝密、机密、秘密、内部和公开。

4.3 秘密以上的信息和数据为保密信息和数据。

4.4 信息和数据的保密等级由数据所属部门负责确定。在确定密级时，须同时确定保密期限。

航空航天工业部 1993-03-30 批准　　1993-10-01 实施

5 机房及设备安全

5.1 机房设施及计算机系统的安全，按 QJ 1236 第 3、4、5 章的规定执行。

5.2 进口的关键设备及软件投入运行前，须请安全保卫部门组织技术安全检查，确认合格后方可投入运行。

5.3 机房的建设、改造应将安全保密工作纳入计划。

5.4 机房必须建立一套严格的安全保密规定并有相应的保证措施。

6 传输安全

6.1 网络运行管理部门应设专人对航天 OIS 计算机网络的安全实施管理、监督与控制，未经网络运行管理部门批准，任何人不得改变网络配置及网络中的数据。

6.2 网络应具备存储加密、传输加密、存取控制及验证等安全功能。

6.3 保密信息必须加密传输，不得以明文的形式传输，密钥至少每三个月更换一次。

6.4 绝密信息和数据一般禁止在航天 OIS 计算机网络上传输，如有特殊需要，需事先报安全保卫部门批准，在对数据本身采取特殊加密处理后方可上网，并严禁滞留在网络内。

7 终端安全

7.1 申请安装终端应由使用单位负责安全保密的人员事先检查终端安装地点和环境，确认符合 QJ 1236 中 9.2.1 条～9.2.3 条的规定后，由办公主管部门批准安装。

7.2 对特定的终端设备，应限定操作人员资格，其方法有：采用口令、识别码等资格认定或设置终端设备钥匙等。

7.3 联机终端使用部门应有专人负责管理。

7.4 使用联机终端必须先征得管理人员同意后，方可使用。

7.5 使用终端要严格执行操作规程，不得随意改变联机终端软件及系统软件设置和硬件连接及配置。

7.6 用户对终端停止操作，超出规定的时间 5～15min 后，系统自动对终端注销。

7.7 使用人员离开终端时，必须退出联网状态。

7.8 入网终端必须采取病毒防范措施。

7.9 在使用过程中如发生失泄密或安全事故，应保护现场并及时向办公主管部门和安全保卫部门报告，不得擅自进行处理。

7.10 终端的电磁辐射应在规定的标准之内，否则应采取屏蔽、相关电磁干扰源、距离防护等措施。

8 存储安全

8.1 保密信息和数据的存储、使用与管理按下列规定执行：

a. 绝密信息和数据严禁存储在计算机系统中;

b. 系统打印输出的保密信息应按相应密级文件的管理规定进行保管和使用;

c. 带有保密信息和数据的废旧打印纸和废旧记录媒体，应按相应密级文件销毁的要求及时销毁。

8.2 所有系统软件、应用软件、信息和数据必须备份，重要的信息和数据要双备份。

8.3 磁盘、磁带等媒体应存放在防火、防电磁辐射的铁柜中保存。

8.4 所有存储的文件、数据必须定期检查和拷贝，并确保存有保密信息的记录媒体的安全。

8.5 保密信息必须有可读的密级和保密期限标志，且密级和保密期限标志应与相应的文件一致，并在整个处理过程中同时存在。

9 软件安全

9.1 软件开发

9.1.1 航天 OIS 计算机网络上运行的软件系统应具备完善的检查跟踪功能，能够记录密码使用率、终端操作、使用者的用户码、联机与脱机时间。

9.1.2 应用软件开发必须增加必要的、完善的安全存取控制功能，防止用户越权存取信息，对非授权使用者可自动关闭终端。

9.1.3 根据数据密级和保密时效的期限，选择相应强度的密码算法，具体算法按 QJ 1877 中第 5 章的规定执行。

9.1.4 应用软件在正式运行之前，必须经过至少三个月的试运行，以考核包括安全保密在内的软件的各种性能。

9.1.5 应用软件未经考核或安全保密措施不健全的，不得在航天 OIS 计算机网络中正式运行。

9.2 安全控制

9.2.1 使用操作系统和数据库管理系统所提供的安全控制功能，必要时可追加一些安全措施，如使之具备监视和阻止各种非法访问活动、记录非法活动证据以及对事故、非法行为进行报警的功能。

9.2.2 信息处理过程中的各环节，必须建立相应的安全保密措施，防止信息被非法故意或自然地损害，保证数据完整和安全。

9.2.3 计算机系统应建立密钥产生、管理和分配办法。

9.2.4 应在计算机内对口令加密存储。

9.2.5 口令字设置与保护按下列规定:

a. 口令字的设置按 QJ 1877 中 6.1.1 条的规定执行;

b. 用户口令的保护按 QJ 1877 中 6.1.2 条的规定执行;

c. 口令字至少每六个月更换一次。

9.3 数据库

9.3.1 数据库必须有严格的存取控制措施，控制用户对数据库的存取权限。

9.3.2 通过实体安全、备份和恢复等多种技术手段来保护数据库的完整性。

9.3.3 数据库应具备从各种故障与事故中进行恢复的能力。

10 人员管理

10.1 人员

10.1.1 凡涉及保密信息的人员，应由使用单位的办公主管部门和人事部门审查确定。

10.1.2 新上岗人员在上岗前，须经过安全保密教育与技术培训，经考核合格者方可承担工作。

10.1.3 定期对系统中的所有工作人员（尤其是关键岗位）进行安全保密教育，并从政治思想、业务水平、工作表现等方面进行考核，考核不合格者不得上岗工作。

10.1.4 对不适合接触保密信息的人员，应及时调离，并及时对系统采取相应措施，如：更换密钥、用户码及口令等。

10.2 人员授权

10.2.1 系统管理员在收到办公主管部门和安全保卫部门的书面审批报告后，根据用户可接触的密级，负责为其建立和修改用户码、授予相应的使用权限，并将审批报告登记备案。

10.2.2 除系统管理员和系统操作员外，其他人员均不得在控制台进行操作。

10.2.3 未被授权的用户，严禁使用航天 OIS 计算机网络内的保密信息，严禁存取授权之外的信息。

10.3 职责

10.3.1 系统中各类人员有责任保护航天 OIS 计算机网络的保密信息不泄露给他人。

10.3.2 系统中各类人员严禁超出自己的职权范围，使用他人的用户码进行操作、打开他人存储的文件进行非法使用。

10.3.3 系统设计人员、管理人员和操作人员有为用户保密的义务。未经用户同意，不得使用用户的账号进行操作。

11 安全保密监督

11.1 安全保密监督应包括对设备选型、设备进口、应用系统开发、维护管理、人员管理、和技术防范措施等方面。

11.2 各信息中心、节点和终端用户须设安全保密负责人，并接受上级安全保卫部门的指导。

11.3 安全保卫部门、办公主管部门和终端安全保密负责人应依照国家有关计算机的安全政策、标准、法规，对计算机的安全管理工作进行监督、检查和指导。

11.4 对在安全保密过程中发现的重大问题应及时报告，由上一级办公主管部门和安全保卫部门进行调查并按有关规定处理。

11.5 对系统的不安全因素，安全保卫部门或安全保密负责人应提出改进的建议，对不及时采取改进措施的，有权责令该部门停机整顿，限期达到安全要求。

附加说明：

本标准由航空航天工业部七〇八所提出。

本标准由航空航天工业部办公厅、保卫司、七一〇所负责起草。