U.S. Department of Transportation
Federal Aviation Administration

# Advisory Circular

Subject: COMPUTER GENERATED/STORED RECORDS
Date: 6/4/93
Initiated by: AIR-200
AC No: 21-35
Change:

1. PURPOSE. This advisory circular (AC) provides information and guidance concerning controls for managing information systems that generate and store records used in the manufacture of products and parts. It describes an acceptable means, but not the sole means, of compliance with the Federal Aviation Regulations (FAR).

2. APPLICABLE RELATED FEDERAL AVIATION REGULATIONS AND ADVISORY CIRCULARS.

a. Part 21, Subpart F, Production Under Type Certificate Only.

b. Part 21, Subpart G, Production Certificates.

c. Part 21, Subpart K, Approval of Materials, Parts, Processes, and Appliances.

d. Advisory Circular 21-1, Production Certificates.

e. Advisory Circular 21-6, Production Under Type Certificates Only.

f. Advisory Circular 21-303.1, Certification Procedures for Products and Parts.

3. DEFINITIONS. For the purpose of this AC, the following definitions apply:

a. Authorizations. Permission granted by management to individuals authorized full or partial admission to restricted access information management systems.

b. Data. A set of alphanumeric and/or graphic characters organized to represent facts or instructions suitable for communicating, interpreting, or processing by a computer.

c. Field. An element of a computer file that may contain data and whose size is controlled by the program.

d. Information Systems. A computer system which is designed to automate a specific function such as records management.

e. Privacy Keys. A password or procedure that allows full or partial access to a restricted information management system.

f. Privacy Locks. A procedure that restricts access to a portion of an information system.

g. Production Approval Holder. A manufacturer who holds one of the following Federal Aviation Admniistration (FAA) production approvals: production certificate, approved production inspection system, parts manufacturer approval, or technical standard order authorization, and controls the design and quality of the product/part thereof.

h. Read Only Capability. The authority given to an individual which allows that person to access or read data in a field without being able to change or enter data.

i. Record. A history of the manufacturing process of a particular item. As used in this AC, a record is not a group of associated data fields or files within an information management system.

j. Write Capability. The authority given to a user which allows that person to enter or change data in a field.

4. DISCUSSION. Production approval holders (PAH) are required by various FAR sections to maintain manufacturing and quality records as evidence that items were produced in accordance with approved design requirements. As the aerospace industry has developed, many PAH's have developed or purchased information systems to generate and store manufacturing and quality records. Advisory Circulars 21-1, 21-6, and 21-303.1 contain information regarding the content of those records. As such, this AC will not discuss what manufacturing and quality records should contain, but rather control mechanisms that should be used when a PAH uses an information system to generate and/or store records of products and parts manufactured to FAR requirements.

5. Computer Generated and Stored Manufacturing and Quality System. A record system will detect and deter unauthorized disclosure, modification, or use of records. Record systems require protection to ensure that an accurate history of the manufacturing process of a part or item exists. An information management system should be protected from intruders. The system should also be protected from employees with authorized access privileges who attempt to perform unauthorized actions. Protection is achieved not only by technical, physical, and personnel safeguards, but also by clearly articulating to all employees organizational procedures regarding authorized system use.

a. Security Principles of Electronic Record Systems. Although information management systems are diverse, common security attributes should be present in all record systems. An acceptable electronic record system should include:

(1) User Identification. Each user of the system should be uniquely identified in the system with an account number or other identification code. This identification code is used to identify who has logged onto the system and is the primary means of verifying access. The information management system should retain the user identification codes entered as a means of verifying the requests made upon the system. This information should be available for review by the system manager.

(2) Authentication of User. There should be a means of verifying that the person entering the user identification code is the authorized individual. Typically, this authentication is through a password known only to the authorized user. This password would allow access to the system only when used together with the user identification code. Passwords should be updated periodically.

(3) Principle of Least Possible Privilege. The authorization capability of the record system should follow the principle that each person is limited to only the information and transaction authority that is required by their job responsibilities. Privacy locks may be used to ensure this principle is followed. The level of access at which information is guarded within the system will depend on the design of the system. Based upon the design of the information management

system, privacy locks and keys may control single data elements or any combinations of data elements. Levels of protection may include the following:

(i) Data-items,

(ii) Data-aggregates,

(iii) Sets,

(iv) Fields,

(v) Files, or

(vi) The complete system.

(4) Relation to Quality Data Responsibilities. The system should ensure that authorization privileges coincide with the responsibilities outlined in the organization's quality control program. For instance, a manufacturing person should not normally have write capability to an inspection acceptance field within a manufacturing record. Additionally, an inspector should not have access to a material review engineer disposition fields within material review records. The system should be capable of assigning each user the specific access authority needed. The various types of authorizations necessary may include:

(i) Read Only Access. Allows the user to read all or specific fields of information, but does not allow any write or data manipulation capability.

(ii) Insert or Write Access Authorizations. Allows the user to enter data into specified fields or series of fields.

(iii) Change Access Authorizations. Allows the user to change entries in specified fields, but does not allow removal of the original entry. This may be accomplished by adding information to a restricted field which is only used when the information in a field must be retained, but the information is not correct. For example, when a part has been rejected by inspection, the rejection history may need to be retained even after the part is repaired. Change authorization may be given to allow a senior inspector the authority to change the inspection status of a reworked item, but the record retains the original rejection indication and the user identification of the individual making the change.

(iv) Delete Access Authorizations. Allows the user to remove entries and leave the fields blank. While authorization to delete information by the user making the entry may be unrestricted, subsequent delete authorization should be closely controlled and possibly issued only to supervisors for deleting incorrect entries by subordinate employees. Subsequent to final approval of a product, information should not be deleted. After approval, incorrect data should be changed rather than deleted.

(v) Security Access Authorizations. The security access authorizations should be retained by the system manager and only exercised when properly executed documents allow their use, such as an approval letter signed by the director of quality.

b. Auditing Mechanisms. The information management system should include mechanisms that detect security breaches. These breaches should include any attempt to circumvent security or modify data without authorization. When such a security breach is detected, the system should alert the security manager and note any fields that have been accessed. The security breach information should be retained within the system until reviewed by the system manager. Security breach logs should be available only to select individuals and be protected from modification or altering of data at all times. Normally the system operator will be warned of unauthorized activity while serious events, such as repeated unauthorized access attempts, may generate alarms at the system level.

c. Protection Against Software and Hardware Destruction. Information system records should be protected from destructive computer programs commonly called computer viruses, which attack or degrade the software. Information management systems should include virus detection programs which ensure that viruses are not introduced into the environment through contaminated software or hardware.

(1) Inventories. Inventories of all software and hardware configurations and locations should be used to ensure unauthorized hardware/software does not enter the computer environment.

(2) Portable Equipment. Portable computer equipment such as laptops represent special risks from destructive software and thus procedures should address their use in the computer environment.

(3) Network Security. Many PAH's use large computer networks with several interacting workstations or terminals. If a large interactive system is used, procedures should address additional protection necessary to control the network. The degree of protection should be defined by the PAH and based upon the complexity and application of the system. Additional protection may be as outlined in the examples cited in paragraph 5.a..

(4) System Back-up. Provisions should be developed for loss of data resulting from system failure. In all cases, lost data must be regenerated. The amount of time between back-ups will depend on the degree of risk the approval holder wishes to accept to re-establish lost information.

d. Media Control. The media upon which information is stored should be carefully controlled and protected. Transportable media such as tapes, disks and cartridges should be stored in secure locations. Media from external sources should be subject to validation to ensure they are from authorized sources. The listing below is not all-inclusive of the types of media available, it only cites examples.

(1) Floppy disks and computer hard drives should not be used for long term storage of quality and manufacturing records. Information that is required to be retained for more than three months should be transferred to optical disks or a magnetic computer, chromium dioxide, or metal particle tapes. An external or electronic labeling system should be used which ensures that individual records can be retrieved.

(2) Magnetic tapes should be tested within six months of use to verify the tape is free of errors and complies with the standards of the National Institute of Standards and Technology. Optimally, new tapes that have been maintained in a cool dry environment should be chosen for storing records. Specific storage criteria for magnetic tapes includes:

(i) Environmental temperatures between 62 and 68 degrees Fahrenheit.

(ii) Relative humidity between 35% and 45%.

(iii) All tapes should be rewound under controlled tension every 3 1/2 years.

(iv) All information that will be retained for more than 10 years should be transferred to new tapes prior to reaching 10 years.

(v) Annually, a statistically valid sample of all tapes should be tested to identify any loss of data. Tapes with 10 or more errors due to storage conditions should have all data transferred to new tapes. If the sample contains defective tapes, all other tapes that might have been affected by the same cause, i.e. poor quality tape, high usage, poor environment, or improper handling should be tested and corrected.

(vi) Smoking, eating, or drinking in the magnetic tape storage or test areas should be prohibited.

(3) Optical disks are not highly sensitive to physical abuse, environmental conditions, or magnetic force fields. Optical disks need only be protected from loss.

(4) Chromium dioxide tapes should be handled like magnetic tapes except for periodic rewinding and cleaning. Although unproven, some industry experts believe that rewinding and cleaning can be destructive to these tapes.

(5) Several types of metal particle tapes will become available in the next few years. It is possible that the metal particles are subject to oxidation. Prior to use of any metal particle tapes for long term storage, the PAH must ensure that the tapes can maintain integrity of the data stored.

(6) Additional information regarding long term storage of electronic media can be found in the National Bureau of Standards Special Publication 500-101 "Care and Handling of Computer Magnetic Storage Media," that is available from the Superintendent of Documents, U.S. Government Printing Office, Washington, D.C. 20402.

e. Documentation. The information management system should be properly documented.

(1) All software programs within the system, including program changes, should be fully documented.

(2) Procedures should be developed that control all data entered into the system. The procedures should address all information management system/human interface activities. The procedures should be kept current.

f. Availability. The computer industry is extremely dynamic concerning the systems that are available for record keeping. If the PAH changes from one system to another, the records that were produced by the old system must remain accessible to the FAA in a usable format. The PAH's documented quality control system should indicate how this accessibility is accomplished.

6. Information Management System Facility Management. The information management system can not be properly protected unless the facilities that house the equipment are properly protected from physical threats and hazards. Areas that should be considered include:

a. Physical Security. Each area in which electronic records will be used should be surveyed for potential physical hazards. Fire and water are two of the most damaging forces in regards to electronic information. Although not all hazards can be eliminated, opportunities for loss can be minimized by careful planning.

b. Environmental Conditions. Procedures should address the environmental (temperature, humidity, static, etc.) conditions of the areas where the record system computers and stored media are located. Manufacturer's specifications provide a good guide for developing procedures.

c. Disaster Recovery. A contingency plan should be developed that will allow recovery of critical system information in case of a disaster, such as a fire. One acceptable method is to have a remote back-up system to which data is regularly transferred.

7. Training. Organizations that have elected to use electronic record systems should train each employee who is involved with any portion of that system. The subject matter and objectives

should vary depending on the employee's level within the organization and job responsibilities. Training should include security awareness, organizational policy, system operation and record storage requirements. Training should be documented and those documents made available for review by the FAA.

Michael Gallagher
Acting Manager, Aircraft
Manufacturing Division


* U.S. G.P.O.:1993-343-273:80056

U.S. Department
of Transportation

**Federal Aviation
Administration**

800 Independence Ave., S.W.
Washington, D.C. 20591

**FORWARDING AND RETURN
POSTAGE GUARANTEED**

Official Business
Penalty for Private Use $300

**BULK MAIL**
POSTAGE & FEES PAID
FEDERAL AVIATION
ADMINISTRATION
PERMIT NO. G-44