APPLICATION & PROCESS:
ELECTRONIC RECORD KEEPING

SECTION 1 GENERAL

1.1 PURPOSE

The purpose of this advisory circular (AC) is to provide guidance for the development and aapproval of electronic records

1.2 STATUS OF THIS AC

This AC is an original issuance.

1.3 BACKGROUND

A. Many operators are developing computer-based record keeping systems, allowing more flexible and efficient maintenance of records.

B. Some computer-based systems offer electronic communications capabilities which benefit both the operator and the CAAP.

1.4 APPLICABILITY

The requirement for CAAP approval before operations in defined RCP airspace applies to operators of Philippine-registered aircraft involved in general aviation, aerial work and commercial air transport.

1.5 RELATED REGULATIONS

The following regulations are directly applicable to the guidance contained in this advisory circular—

- PCAR Part 3, Approved Training Organizations
- PCAR Part 6, Approved Maintenance Organizations
- PCAR Part 9, AOC Certification and Administration
- PCAR Part 11, Aerial Work Operations
- PCAR Part 18, Safe Transportation of Dangerous Goods

1.6 RELATED PUBLICATIONS

For further information on this topic, operators and individuals are invited to consult the following publications—

- Advisory Circulars are intended to provide advice and guidance to illustrate a means, but not necessarily the only means, of complying with the regulations, or to explain certain regulatory requirements by providing informative, interpretative and explanatory material.
- Where a regulation contains the words "prescribed by the Authority," the AC may be considered to "prescribe" a viable method of compliance, but status of that "prescription" is always "guidance" (never regulation).

1) Civil Aviation Authority of the
Philippines (CAAP)

- ♦ AC 00-003, CAAP Generic Certiification Process

- ♦ AC 08-013, Crew Fatigue Risk

- ♦ AC 08-017, Acceptable Required Flight Records

1.7   DEFINITIONS & ACRONYMS

1.7.1   DEFINITIONS

The following definitions apply to this advisory circular—

1) **Authentication.** The means by which a system validates the identity of an authorized user. These may include a password, a personal identification number (PIN), a cryptographic key, a badge, or a stamp.

2) **Computer-Based Record keeping System.** A system of record processing in which records are entered, stored, and retrieved electronically by a computer system rather than in traditional hard copy form.

3) **Computer Hardware.** A computer and the associated physical equipment directly involved in the performance of communications or data processing functions.

4) **Computer Software.** Written or printed data, such as programs, routines, and symbolic languages essential to the operation of computers.

5) **Control.** A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.

6) **Database Management System (DBMS).** A computer software program capable of maintaining stored information in an ordered format, manipulating that data by mathematical methods, and performing data processing functions such as retrieval of data.

7) **Data Entry.** The process by which data or information is entered into a computer memory or storage medium. Sources include manually written records, real-time information, and computer-generated data.

8) **Data Verification.** A process of assuring accuracy of data records by systematically or randomly comparing electronic records with manual data entry documents.

9) **Digital Signature.** Digital signature technology is the foundation of a variety of security, e-business, and e-commerce products. Based on public/private key cryptography, digital signature technology is used in secure messaging, public key infrastructure (PKI), virtual private networks (VPN), web standards for secure transactions, and digital signatures

10) **Electronic Mail.** The transmittal of messages, documents, or other communications between computer systems or other telecommunication channels.

11) **Electronic Record.** A contract, Operation Specification Paragraph (OpSpec), or other record created, generated, sent, communicated, received, or stored by electronic means.

12) **Electronic Signature.** An electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent for electronically identifying individuals entering, verifying, or auditing computer-based records, and checking for authenticity.

♦ An electronic signature combines cryptographic functions of a digital signature with the image of a person's handwritten signature or some other form of visible mark that would be considered acceptable in a traditional signing process, authenticates data, and provides permanent secure user authentication.

13) **Electronic Technology.** Relating to or having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

14) **Modem.** A device that can use existing telephone transmission circuits to transfer information between either two or more computer systems, or computers and remote terminals.

15) **Password.** An identification code required to access stored material. A device intended to prevent information from being viewed, edited, or printed by unauthorized persons.

16) **Proprietary Information.** Information that is the private property of the operator.

17) **Real-Time Record.** Information that is entered into a computer-based record keeping system immediately following the completion of an event or fulfillment of a condition, without first relying on the manual recording of the information on a data entry form.

18) **Records.** Information in a predetermined format that shows that the operator or its personnel have accomplished a particular event, have met certain criteria, or have fulfilled specific conditions required by the regulations.

19) **System Security.** Policies, procedures, and system structures designed to prevent users from gaining access to sections of a database to which they are not authorized access.

20) **Telephone Dial-In Access.** A means of gaining access to a computer system from a remote location through a telephone modem and existing telephone circuits.

21) **User Identification.** A series of alphabetic and/or numeric characters assigned to one or more individuals or organizations for the purpose of gaining access to a computer system and accounting for time usage.

1.7.2 ACRONYMS & ABBREVIATIONS

The following acronyms apply to this advisory circular—

1) **AC** – Advisory Circular

2) **AOC –** Air Operator Certificate

3) **CAAP** – Civil Aviation Authority of the Philippines

4) **CAAP-FSIS** – Flight Standards Inspectorate Service

5) **PCARs –** Philippine Civil Aviation Regulations

6) **PI –** Principal Inspector

1.8 CHARACTERISTICS OF INFORMATION & RECORDS

Organizations may collect and use both information and records in the conduct of operations.

1.8.1 INFORMATION VERSUS RECORD

A. A record is defined as an account which preserves evidence of the occurrence of an event.

B. In general, a record must show—

1) What event occurred;

2) To whom, by whom, when; and

3) Proof of the event's occurrence, such as a certification by signature or by electronic means.

> A system that collects related information for making operational decisions but does not preserve evidence of the event's occurrence **is not** a recordkeeping system.

1.8.2   PROPRIETARY INFORMATION

A. Proprietary information is that information which is the sole property of the organization. The CAAP is not normally concerned with proprietary information.

B. However, if the organization chooses to interweave the records required by the PCAR with their business records, the required information must be readily accessible to the CAAP.

> The CAAP recommends that organizations should contruct their record keeping systems so that they do not include proprietary information.

- For example, if an operator chooses to maintain flight and rest records on a payroll form, the operator must make the record available for inspection.

SECTION 2   GENERAL POLICIES

2.1   HARD-COPY RECORD KEEPING SYSTEM

A. All organizations must have acceptable processes consisting of instructions, forms and training to support the necessary hard-copy record keeping to meet the record keeping requirements of the PCARs.

B. After meeting the requirements for hard-copy records, the organization may make application to replace the hard-copy records process with electronic records processes.

C. Normally the CAAP will require that the raw records used to input to the electronic records system are retained for a period of 3 months to allow confirmation inspections of the primary records accuracy.

> Where the electronic system entry requirements do not rely on input records, the CAAP will require a parallel system of temporary hard-copy records during the validation process.

- This period may be reduced based on the confidence of the CAAP with the quality of the records.

2.2   CATEGORIES OF RECORDS COVERED BY THIS ADVISORY CIRCULAR

A. An CAAP-certificated organization may apply for approval of a computer-based record keeping system that is designed to satisfy—

1) Either all regulatory requirements; or specific

2) Specific regulatory requirements, such as training records.

B. The operator may apply for one or more of the following categories of records to be maintained by the computer-based record keeping system—

- Airman training records (including pilot, flight engineer, flight navigator, flight attendant, flight instructor, check airman, and aircraft dispatcher training records)

- Aircraft qualification records (including aircraft type ratings, proficiency checks, competency checks, and line checks)

- Flight time limitation and rest requirement records

- Medical qualification records (when applicable)

- Route, "special airport," and area qualification records
- Operating experience (OE) and/or operating familiarization records
- Pilot recency of experience records
- Check airman, aircrew program designee (APD), and school designated examiner (SDE) designations or authorizations
- Special training or testing requirements
- Aircraft listings
- Load manifests, dispatch/flight releases
- Communication records

2.3   RECORD RETENTION

The record retention will never be less than that specified by the PCARs.

2.4   CAAP ACCESS TO THE RECORDS

A. CAAP inspector personnel assigned to the operator should be provided with an access level which allows unrestricted data retrieval of all records required by the PCAR.

B. If the operator elects to use the computer record keeping system's capability for electronic designation of a CAAP-designated representative (such as a check airman), an appropriate level of access should be provided to the PI or a designated representative to allow necessary data entries.

C. Any document/information in an electronic format must remain accessible to all persons who are entitled to access by statute, regulation, or rule of law—

1) For the period required by such statute, regulation, or rule of law; and

2) In a form that is capable of being accurately reproduced for later reference, whether by transmission, printing, or otherwise.

SECTION 3   CAAP APPROVAL PROCESS

3.1   GENERAL

A. The CAAP evaluation of a computer-based record keeping system will ensure that the proposed system provides a means of maintaining records that are—

> The CAAP will follow the general five-step approval process described in AC 00-004 when approving an electronic record keeping system.

1) Accurate;

2) Timely; and

3) Reliable records.

3.2   ANNOUNCING INTENT TO USE ELECTRONIC RECORD KEEPING

A. Organizations and operators intending to use electronic record keeping should consult with the CAAP before implementing an electronic system.

B. To obtain CAAP approval, the approved organization or operator must submit a

> Refer to Appendix A of this circular for a sample letter.

letter of intent to the CAAP-FSIS describing the proposed system and include the proposed section or revision to the operator's manual.

3.3   CAAP PROCESSING

A. The application and supporting documents will be reviewed by the assigned CAAP inspector as a part of the electronic record keeping proposal.

B. If the proposed electronic hardware and computer software system meets the elements of this AC, the inspector will make the appropriate entry on the operator's operation specifications.

C. For a general aviation operator, the regulations do not require CAAP approval; however, if the general aviation operator wants to submit its electronic system to the CAAP, the CAAP will review the operator's proposed procedures.

D. If the procedures are acceptable, the CAAP will provide the operator with a letter of acceptance.

E. Through out the approval process, PI shall ensure that any operator that requests approval of a computer-record keeping system retains data entry forms or other pertinent nonelectronic records in a parallel record system.

F. The PI shall ensure that all required records continue to be maintained while the computer-based record keeping system is being installed, tested, and evaluated and data entry personnel are being trained to recognize regulatory terminology and requirements

SECTION 4   REQUIRED OPERATOR APPLICATION

4.1   LETTER OF APPLICATION

A. The letter of application must contain the following information—

1) A general description of the proposed computer-based record keeping system (including the facilities, hardware, and software to be utilized)

2) The data backup system to be used

3) Access and security procedures for both the operator and FAA personnel

4) Basic procedures for data entry personnel

5) A general description of any special procedures and capabilities

6) Digital or electronic signature type(s) and processes to be used (if applicable)

B. A copy of the instructions manual for the record keeping software must be provided with the application.

> This manual may be provided in a digitial form that is readable by CAAP software.

4.2   DESCRIPTION OF ELECTRONIC SYSTEM & PROPOSED MANUAL CHANGES

A. The electronic system description should explain how the electronic record keeping will be used in the operator's maintenance and operational activities.

B. The proposed manual section or revision should clearly state who in the organization has authority and the overall responsibility for implementing, modifying, revising, and monitoring the electronic record keeping computer software.

Section 5   Electronic Record Keeping Systems

5.1   Attributes of an Acceptable Electronic Record Keeping System

A. The key attributes of an electronic system are acceptable—

1) Security; and

2) Procedures.

B. These key attributes must be considered and addressed in the operator's manual or in the instructions for the use of the system when constructing an electronic record keeping system to meet the operational and maintenance requirements addressed in this AC.

> The operator's policy, instructions and procedures for use of the system must be made immediately available to each individual responsible for using the system.

5.2   Security

The security of the electronic system is paramount for the record keeping system.

1) The electronic system should protect confidential information.

2) The system should ensure that the information is not altered in an unauthorized way.

3) A corresponding policy and management structure should support the computer hardware and computer software that delivers the information.

5.3   Procedures

Before introducing an electronic record keeping system, computer procedures must be incorporated into the operator's manual or in the directions for the system to include the following—

1) Procedures for making required records available to both the CAAP inspector personnel.

> ● The CAAP must be able to review the records and information at their respective offices when necessary and on request.
> ● Persons or entities can fulfill this request in many ways, i.e., floppy disk, paper copy, etc.

(a) If the computer hardware and software system is not compatible with the CAAP system, the organization will provide an employee or representative to assist.

(b) This individual must be familiar with the computer system and assist in accessing the necessary computerized information.

(c) This procedure and computer system must be capable of producing paper copies of the viewed information at the request of the CAAP authorized personnel.

2) Procedures for reviewing the computerized personal identification codes system to ensure that the system will not permit password duplication.

3) Procedures for auditing the computer system every 60 days to ensure the integrity of the system.

♦ A record of the audit should be completed and retained on file as part of the operator's record retention requirements. This audit may be a computer program that automatically audits itself.

4) Audit procedures to ensure the integrity
    of each computerized workstation.

> If the workstations are server-based and contain no inherent attributes that enable or disable access, there is no need for each workstation to be audited.

5) Procedures describing how the operator
    will ensure that the computerized
    records are transmitted in accordance
    with the appropriate regulatory
    requirements to customers or to another operator.

> The records may be either electronic or paper copies.

6) Procedures to ensure that records required to be transferred with an aircraft are in a format (either electronic or on paper) that is acceptable to the new owner/operator.

7) Guidelines for authorized representatives of the owner/operator to use electronic signatures and to have access to the appropriate records.

8) A description of the training procedure and requirements necessary to authorize access to the computer hardware and software system.

    ♦ Recognizing that the details will vary with the different individuals who need access, the training description may simply be part of the position description.

    ♦ Its location should be referenced in the manual)

5.4   CONTROL OF TRANSFERABLE RECORD

A. A system satisfies "control," and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that—

1) A single authoritative copy of the transferable record exists which is unique, identifiable, and unalterable (except as otherwise provided in this AC).

2) The authoritative copy identifies the person asserting control as—

    ♦ The person to whom the transferable record was issued; or
    ♦ The person to which the transferable record was most recently transferred, if the authoritative copy indicates that the transferable record has been transferred.

3) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

4) Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

5) Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

6) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

5.5   DATABASE INSTRUCTIONS MANUAL

A. The organization must provide a working procedures manual for day-to-day guidance and training for the operator's employees.

● This manual should also be provided with the application approval.

● One copy will be retained by the CAAP as a reference document for their use in accessing the record keeping system.

B. This manual must include guidance in the automated recordkeeping system structure and instructions for using computer commands for such operations as—

1) Data entry;

2) Data processing;

3) Data retrieval; and

4) Report generation.

C. This manual should address system security procedures and responsibilities, including identification of personnel charged with various levels of—

1) Data entry;

2) Data verification and correction;

3) Data audits; and

4) Quality control.

D. This manual should also identify individuals with the authority to issue user access codes and passwords.

5.6 BACKUP CAPABILITY

A. The organization must have established a backup capability to generate a complete set of duplicate records, either electronic or nonelectronic.

> ⚠️ These records should be stored in a location separate from the main information storage facility.

B. These records may be stored in any form acceptable to the PI, including magnetic tape, magnetic or optical disk, microfiche, or printed records.

C. The organization shall back up data as frequently as appropriate to the operator's level of operations and system complexity.

- For example, a large organization may perform a simultaneous on-line data backup, while a smaller organizationr may perform backups at less frequent intervals.

5.7 QUALITY ASSURANCE

A. The organizations' electronic record keeping systems must be included in the organizations' quality assurance programs.

B. The associated audit procedures (as provided in checklists) must be adequate to assure the accuracy of the database.

C. The frequency and scope of these procedures should reflect the complexity of the computer-based recordkeeping system and the size of the database.

SECTION 6 ELECTRONIC SIGNATURES

6.1 GENERAL

A. This section outlines that methods by which electronic signatures may be used to certify records.

> - The CAAP continues to accept paper documents to satisfy current regulatory requirements.
> - The operator now has the option to use electronic signatures for electronic recordkeeping systems.

- Handwritten signatures are still acceptable used on any required record, record entry, or document.
- Organizations may exercise the option to print out records and certify them.

B. The electronic signature's purpose is identical to that of a handwritten signature or any other form of signature currently accepted by the CAAP.

C. The handwritten signature is universally accepted because it has certain qualities and attributes that should be preserved in any electronic signature.

> It is critical that an electronic signature should possess those qualities and attributes that guarantee a handwritten signature's authenticity.

6.2   FORMS OF ELECTRONIC SIGNATURES

A. An electronic signature may be in the following forms—

- A digital signature
- A digitized image of a paper signature
- A typed notation
- An electronic code

B. Any other unique form of individual identification that can be used as a means of authenticating a record, record entry, or document may be considered by the CAAP for approval.

C. Not all identifying information found in an electronic system may constitute a signature.

- For example, the entry of an individual's name in an electronic system may not constitute an electronic signature.
- Other guarantees equal to those of a handwritten signature should be provided.

6.3   ELEMENTS OF AN ACCEPTABLE ELECTRONIC SIGNATURE

An electronic signature must be part of a well-designed program. This program should, at a minimum, consider the following—

6.3.1   UNIQUENESS

A. An electronic signature should retain those qualities of a handwritten signature that guarantee its uniqueness. A signature should identify a specific individual and be difficult to duplicate.

B. A unique signature provides evidence that an individual agrees with a statement.

C. An acceptable method of proving the uniqueness of a signature is by using an identification and authentication procedure that validates the identity of the signatory.

> An electronic system cannot provide a unique identification with reasonable certainty unless the identification is difficult for an unauthorized individual to duplicate.

- For example, an individual using an electronic signature should be required to identify himself or herself, and the system that produces the electronic signature should then authenticate that identification.

D. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes.

- These codes could be encoded onto badges, cards, cryptographic keys, or other objects.

E. Systems using PINs or passwords also are an acceptable method of ensuring uniqueness.

- Additionally, a system could use physical characteristics, such as a fingerprint, handprint, or voice pattern, as a method of identification and authorization.

6.3.2   SIGNIFICANCE

A. An individual using an electronic signature should take deliberate and recognizable action to affix his or her signature.

B. Acceptable, deliberate actions for creating a digital electronic signature include, but are not limited to, the following—

- Badge swipes
- Signing an electronic document with a stylus
- Typing specific keystrokes
- Using a digital signature

6.3.3   SCOPE

A. The scope of information being affirmed with an electronic signature should be clear to the signatory and to subsequent readers of the record, record entry, or document.

B. Handwritten documents place the signature close to the information to identify those items attested to by a signature. However, electronic documents may not position a signature in the same way.

> It is important to clearly identify the specific sections of a record or document that are affirmed by a signature from those sections that are not.

C. Acceptable methods of marking the affected areas include, but are not limited to—

- Highlighting
- Contrast inversion
- Use of borders
- Use of flashing characters

D. Additionally, the system should notify the signatory that the signature has been affixed.

1) The user should be asked to ensure that the identified material is, in fact, what is being signed for after affixing the signature.

2) The user also should be able to retrieve a report listing all places where his or her digital electronic signature has been applied.

> The CAAP concern is with the accuracy of the record and that the signatory is fully aware of what he or she is signing.

E. The computer technology in use will ensure the signature is secure.

6.3.4   SIGNATURE SECURITY

A. The security of an individual's handwritten signature is maintained by ensuring that it is difficult for another individual to duplicate or alter it.

B. An electronic signature should maintain an equivalent level of security.

C. An electronic system that produces signatures should restrict other individuals from affixing another individual's signature to a record, record entry, or document.

> Such a system enhances safety by preventing an unauthorized individual from certifying required documents, such as a maintenance release. .

1) A corresponding policy and management structure must support the computer hardware and software that and software that delivers the information.

2) Signature authenticity/verification—

(a) Through control and archives, the computer software should determine if the signature is genuine and if the individual is authorized to participate.

(b) This can be accomplished by comparing the signature to a public key archive or some other means.

(c) This capability should be an integral part of the computer software.

3) Archiving electronically signed documents is critical to the approval.

♦ Since no paper document with an ink signature exists, a means of safely archiving electronically signed documents should be part of any electronic signature computer software.
♦ This will provide for future authentication.

4) The system should contain restrictions and procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment.

> ⚠ This should be done immediately upon notification of the change in employment status. .

5) Procedures should be established allowing the organization to correct documents that were electronically signed in error.

♦ The signature should be invalidated anytime a superseding entry is made on the same document.
♦ The entry should be voided but remain in place.
♦ Reference to a new entry should be made and electronically signed and dated.

6.3.5   NON-REPUDIATION

A. An electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document.

> The more difficult it is to duplicate a signature, the likelier the signature was created by the signatory.

B. The system's security features that make it difficult for others to duplicate signatures or alter signed documents usually ensure that a signature was indeed made by the signatory.

1) Many off-the-shelf computer software packages, such as Adobe Acrobat, contain a self-sign utility.

2) Although such computer software can provide an electronic signature for individuals or a group of individuals participating in an electronic signature program, a self-sign utility by itself cannot be used.

3) However, it can become the basis of a digital signature program if the public and private keys are issued and controlled by a trusted third party.

6.3.6   TRACEABILITY

An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

6.4   OTHER ACCEPTABLE FORMS OF SIGNATURE/IDENTIFICATION

A. Although this AC specifically addresses electronic signatures, other types of signatures, such as a mechanic's stamp, may also be acceptable to the CAAP If identification other than a handwritten signature is used, access to that identification should be limited to the named individual only.

● For example, the individual should secure a mechanic's stamp when it is not in use.

B. Similarly, a computer entry used as a signature should have restricted access that is limited by an authentication code that is changed periodically.

> Although a signature may take many forms, the CAAP emphasizes that not all electronic entries may satisfy the criteria to qualify the entry as an acceptable signature.

C. Access to issued stamps or authentication codes should be limited to the user.

6.5 COMPLIANCE WITH OTHER REGULATORY REQUIREMENTS

A. Although the CAAP now permits the use of electronic signatures to meet certain CAAP operational and maintenance requirements, any computer hardware used to generate the required documents and records must continue to meet current regulatory requirements.

B. A proper signature affixed to an improperly created document still results in a document that does not meet regulatory requirements.

C. Methods and procedures used to generate an electronic signature must therefore meet all regulatory requirements for a recordkeeping system to be used by owners, operators, or maintenance personnel.

> The more difficult it is to duplicate a signature, the likelier the signature was created by the signatory.

D. Electronic signatures may not be considered acceptable in other areas covered by the PCARs having more specific applicability (i.e., legal depositions and various other applications).

> For the present, electronic signatures will only be approved to satisfy the maintenance and operational requirements specified earlier in this AC.

The Remainder Of This Page Intentionally Left Blank

APPENDIX A

Sample Letter Of Intent For General Aviation Operators

[Requester Letterhead]

To: CAAP Flight Standards Inspectorate Service

From: [Requester]

Date:

Subject: Use of Electronic Record Keeping System

This letter is to inform you that [requester] intends to use an electronic recordkeeping) system for [describe what the system will be used for]. This system has been established using the guidelines outlined in Advisory Circular 00-003.

This organization intends to implement the system on [date].

Company facilities, equipment, and personnel are available for your review and/or inspection at [address] on [date]. Please contact [name] at [telephone] to arrange a visit to review the system and to discuss any CAAP concerns.

Thank you in advance for your assistance in this matter.

Sincerely,

[Requester]

End of Advisory Circular

RAMON S. GUTIERREZ
Director General

Date of Issue : 23 September 2011