	Company Name ETHIOPIAN CIVIL AVIATION AUTHORITY	Document No. ECAA-AC-GEN005	
Document Title:	Advisory Circular on Electronic Signatures, Electronic Recordkeeping and Electronic Manual Systems	Issue No. 1	Page No. Page 1 of 30

ELECTRONIC SIGNATURES, ELECTRONIC RECORDKEEPING and ELECTRONIC MANUALS

This Advisory Circular (AC) provides standards and guidance for electronic signatures, electronic recordkeeping, and electronic manual systems. Electronic recordkeeping systems may be used to generate many types of records (e.g. aircraft maintenance records, maintenance task cards, dispatch release, flight release, and/or airworthiness release, load manifests, pilot training records.). This AC describes an acceptable means, but not the only means, for a certificate holder to utilize an electronic signature, electronic recordkeeping, and electronic manual systems. Hence, the certificate holder intending to implement electronic signatures, electronic recordkeeping, and electronic manual systems shall, at a minimum, meet the standards set out in this AC.

Approved by:

Signature: Woserayish Hunegnaw (CoL)
Director General

Effective Date: 19th September 2019

Ethiopian Civil Aviation Authority

Federal Democratic Republic of Ethiopia
CIVIL AVIATION AUTHORITY

TABLE OF CONTENTS

1. General. Pursuant to Article 92 No. 2 of Civil Aviation Proclamation 616/2008 the Director General of the Ethiopian Civil Aviation Authority may, from time to time, issue directives containing rules and standards necessary for the proper implementation of the Proclamation. This Advisory Circular contains information about standards, practices and procedures acceptable to ECAA.

2. Purpose. This Advisory Circular is issued to provide guidance and mandatory information on the use of electronic signatures, electronic recordkeeping, electronic documents such as manuals, as an alternative to paper-based systems. The Certificate holders engaged in civil aviation operations and intending to implement electronic signature, electronic record-keeping or electronic manual systems shall meet, at a minimum, the standards set out in this Advisory Circular.

3. Applicability. This Advisory Circular applies to Certificate holders conducting civil aviation operations and intending to implement electronic documentation systems.

4. Change Information. This is the first issue of this Advisory Circular.

5. Effective Date. This Advisory Circular is effective from 13th September 2019.

6. References.

ECAA Advisory Circular ECAA-OPS/AWS008 Electronic Flight Bags
Part 3 — Approved Training Organizations
Part 6 — Approved Maintenance Organizations
Part 8 — Operations
Part 9 — Air Operator Certification and Administration

7. BACKGROUND.

7.1 This Advisory Circular highlights the requirements arising from the evolving, real-time needs of the aviation industry with regard to the use of electronic signatures, electronic record-keeping and electronic manual systems.

7.2 ECAA supports the use of electronic systems such as electronic signatures, electronic recordkeeping and electronic manuals. Such systems may now be used to generate and sign off aircraft records, such as maintenance task cards, aircraft maintenance records, certificate of release to service statement and flight test reports. These can be authenticated using an electronic signature and thus enabling a paperless system. The electronic system(s) may also be used for maintenance personnel training records.

7.3 The electronic system(s) may also be used to generate flight operations records and aircraft technical log data such as defect entry and rectification, flight times, Minimum Equipment List (MEL), Deferred Defects List (DDL), loading or manifest, dispatch release, flight test reports, pilot training records, etc.

7.4 A holder of ECAA certificate intending to use electronic system(s) in lieu of paper system(s) shall ensure that he has established system level capability at the organizational level reflected in chapter 1below.

Chapter 1 Definitions and Organizational Level Capabilities.

1.1. Definitions.

The following terms as used in this Advisory Circular have the meaning stated.

a. 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 swipe, or a stamp, etc. These means may be combined (e.g., a cryptographic card and a PIN) for increased confidence in the identity of the system user.

b. Computer-Based Recordkeeping System. A system of record processing in which records are entered, maintained, archived, and retrieved electronically. The term computer-based recordkeeping system is synonymous with electronic recordkeeping system.

c. Data Backup. Use of one of several recognized methods of providing a secondary means for archiving records, separately from the original or primary. This can be used to reconstruct the format and content of electronically stored records in case of loss of, failure of, or damage to the primary recordkeeping system.

d. 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.

e. Data Verification. A process of ensuring accuracy of data records by systematically or randomly comparing electronic records with manual data entry documents.

f. 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.

g. Digital Signature. Cryptographically generated data that identifies a document's signatory (signer) with date and time, and certifies that the document has not been altered. The result of digital signature when properly implemented provides the services of original authentication, data integrity, and signer non-repudiation. Digital signature technology is based on public/private key cryptography, digital signature technology used in secure messaging, public key infrastructure (PKI), virtual private network (VPN), web standards for secure transactions, and electronic digital signatures.

h. Electronic Manuals. Certificate holder manuals including operational and/or maintenance manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, Internet/Intranet-based, or in other various forms of electronic media, to include commercial off-the-shelf portable electronic device (PED) hardware (e.g., laptop, tablet, phone, etc.). Electronic manuals may consist of accepted or approved data and/or reference data used in aircraft maintenance or operations.

i. Electronic Record. A record (including contracts and OpSpecs) created, generated, sent, communicated, received, or stored by electronic means.

j. Electronic Recordkeeping System. A system of record processing in which records are entered, signed, stored, and retrieved electronically by a computer system rather than in the traditional hardcopy or paper form. The term electronic recordkeeping system is synonymous with computer-based recordkeeping system.

k. Electronic Signature. The electronic equivalent of a handwritten signature. It is an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by an individual with the intent to sign a record. It electronically identifies and authenticates an individual entering, verifying, or auditing computer-based records. An electronic signature combines cryptographic functions of digital signatures with the image of an individual's handwritten signature or some other visible mark considered acceptable in a traditional signing process. It authenticates data with a hash algorithm, provides permanent, secure user-authentication, and is considered to be the legally binding equivalent of the individual's handwritten signature. In this Advisory Circular, the term "electronic signature" refers to either electronic signatures or digital signatures. The specific electronic signature used depends on the end user's preference and the system application.

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

m. Letters of Authorization (LOA). Document/letter issued to certificate holders by ECAA authorizing use of electronic systems.

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

o. Private Key. A key pair used to create a digital signature.

p. Public Key. A key pair used to verify a digital signature.

q. Real-Time Record. Information that is entered into a computer-based recordkeeping 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.

r. Record. Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.
s. Signature. A mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation, and to authenticate a record entry. A signature must be traceable to the individual making the entry, and it must be handwritten or part of an electronic signature system or other form acceptable to the ECAA.
t. System Security. Policies, procedures, and system structures designed to prevent users from gaining unauthorized access.
u. User Identification. A series of alphanumeric characters assigned to an individual for the purpose of gaining access to a computer system and accounting for time usage.

1.2 ORGANIZATIONAL LEVEL CAPABILITIES.

1.2.1 Before introducing electronic system(s) for signatures, recordkeeping or manuals Certificate holders shall establish a program capable of implementing such technologies. As a minimum, the program shall broadly include the following key safeguards:

(a) Identification of key personnel in the organization with authority and overall responsibility for implementing, modifying, revising, and monitoring the electronic system. There shall be a compliance manager or equivalent personnel responsible for ensuring the integrity and security of the electronic system and that the process is followed. In addition, there shall be a system to allow identification on who is authorized to use the electronic system and for what purposes.

(b) The system shall ensure that the information is not altered in an unauthorized way and should include data alteration traceability features. A corresponding policy and management structure should support the computer hardware and computer software that delivers the information.

(c) To provide quality assurance, there shall be an auditing process and plan to ensure the requirements for an electronic system continuity to be met and ensure the integrity of the system. A record of the audit should be completed and retained on file in accordance with an organization's record retention policy. This audit may be a computer program that automatically audits itself. The audit procedures shall also contain how and when to submit any changes to the process to ECAA for acceptance and approval prior to implementation.

(d) Procedures for making maintenance records available for review by the ECAA. This procedure and computer system must be capable of producing paper copies of the viewed information at the request of the ECAA.

(e) Procedures describing how electronic signatures will be used as it relates to all the elements that are associated with the use of electronic signatures. Procedures to generate passwords and personal identification codes that ensure the system will not permit password duplication.

(f) Procedures describing how an organization will ensure that the computerized records are transferable and are transmitted in accordance with the appropriate regulatory requirements to customers or to another Organization. The records may be either electronic or paper copies.

Procedures to ensure that records required to be transferred with an aircraft are transferable and in a format (either electronic or on paper) that is acceptable to the new owner/operator.
(g) Procedures for data backup and recovery.
(h) Details relating to the training requirements shall be defined. The program shall include procedures for on-going training of personnel. If the technologies used are novel or first-of-its-kind, training shall also be provided for ECAA officers.
(i) The electronic system shall be developed based on the following technical specifications:
(i) ATA Spec 2000 e-business Specification
(ii) ATA iSpec 2200 Information Standards for Aviation Maintenance
(iii) ATA Spec 2300 Data Exchange Standard for Flight Operations
(iv) ATA Spec 42 Aviation Industry Standards for Digital Information Security
(v) S1000D International Specification for Technical Publications Using a Common Source Database
(vi) ARINC-811 Commercial Aircraft Information Security Concepts of Operation and Process Framework
(vii) RTCA/EUROCAE documents DO-355/ED-204 - Information Security Guidance for Continuing Airworthiness

1.2.2 The certificate holder shall explain in its manual how electronic system(s) would be used or applied throughout their operation. There shall be a description of the hardware and software capabilities for applications of the electronic system(s). The description shall also include system support of any computer hardware or software that is part of the electronic system(s). Chapters 2, 3 and 4 provide more details about required standards and security elements for an electronic signature, electronic recordkeeping and electronic manual systems.

CHAPTER 2. ELECTRONIC SIGNATURES

2.1. ELECTRONIC SIGNATURE. Electronic Signature is defined as 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 to sign the record.
NOTE: Throughout this AC, the term electronic signature refers to either electronic signatures or digital signatures. The specific electronic signature used depends on the end user's preference and the system application. The onus is on the certificate holder to assess whether the means of identification and authentication (e.g. user-ID and password, one-time or dynamic password, biometrics, digital certificates) used are adequate, suitable and effective for the system.
a. General. The electronic signature's purpose is identical to that of a handwritten signature or any other form of signature currently accepted or approved by the ECAA; therefore, electronic signatures must possess those qualities and attributes that guarantee a handwritten signature's authenticity.

NOTE: Electronic signatures should only be used to satisfy requirements relating to this AC. They may not be considered acceptable in other areas covered by national regulations having more specific applicability (e.g., legal depositions).

b. Types of Electronic Signatures. Electronic signatures may appear in various formats. No matter the format, they must meet the legal requirements of electronic signing that appear in subparagraph 2-1c.

Examples of electronic signature formats include, but are not limited to:

- A digitized image of a handwritten signature that is attached to an electronic record;
- An electronic code (e.g., a secret code, password, or personal identification number (PIN)) used by a person to sign the electronic record;
- A unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan; or
- A digital signature.

c. Electronic Signature Standards. Electronic signatures should meet the following criteria to be considered legally binding.

(1) A person (the signer) must use an acceptable electronic form of signature.

(2) The signature must be unique to the signatory.

(3) There must be a means to identify and authenticate a particular person as the signer.

(4) The electronic form of signature must be executed or adopted by a person with the intent to sign the electronic record to indicate a person's approval or affirmation of the information contained in the electronic record.

(5) The electronic form of signature must be attached to or associated with the electronic record being signed.

(6) The signature must be permanent and the information to which it is attached must be unalterable without a new signature.

(7) There must be a means to preserve the integrity of the signed record.

(8) A valid electronic signature must prevent the signatory from denying that he or she affixed a signature to a specific record, document, or body of data (non-repudiation).

d. Digital Electronic Signatures. Digital signatures are electronic signatures that incorporate encryption and decryption technology. Digital signatures that use this technology are typically the most secure because of the controls that are inherent with the technology itself.

(1) Digital Cryptography. Digital signature technology is the foundation of a variety of security and electronic transactions. Digital signature technology is based on Public and Private Key Infrastructure (PKI) cryptography. PKI cryptography is a class of cryptographic algorithms which require two separate keys, one of which is secret (private) and one of which is public. Although different, the two parts of this key pair are mathematically linked. The public key is used to encrypt plain text or to verify a digital signature; whereas the private key is used to decrypt cipher text and to create a digital signature. To ensure the authenticity of a digital signature, PKI must incorporate the use of a digital certificate to authenticate the signatory's identity. Once approved, subsequent use of the individual's digital certificate can be trusted. While self-issued certificates are the easiest to implement and manage, digital certificates using

PKI (acceptable to ECAA) can also be issued and managed using a PKI consisting of servers, databases, cryptographic applications, and policies. The PKI ensures that digital certificates are used under the sole control of an issuing organization, and can be revoked or suspended at a later date if an individual's status changes. Digital certificates using PKI can be issued and managed by a central department or person within an organization, or by a trusted third party, preferably an accredited Certification Authority as defined in the e-business standards. A digital certificate is issued by a trusted third party to establish the identity of the signatory. The third party who issues the digital certificate is known as a certificate authority (CA). The Certification Authority (CA) assumes the responsibility and liability of vouching for an individual's identity. The general features of a reliable digital signature and duties of subscribers shall be defined clearly by a certificate holder.

(a) Public Key. A public key in a digital signature encrypts the digital signature itself and essentially converts it to a series of numbers and letters that are nearly impossible to duplicate. The encrypted data in a digital signature public key can be accessed by anybody; hence the term "public" key. However, only the individual with the private key can turn the encrypted data into a digital signature. Examples of public keys include smart cards, digital tokens, access badges, or a user ID.

(b) Private Key. A Private Key is used by the individual signatory to decrypt the public key data and turn it into a digital signature. Examples of private keys are unique user name/password/access code combinations. A private key must be under the sole control of the person using it. The signatory must keep the private key secret and stored in a protected environment.

(c) Digital Certificate and CA. The digital certificate verifies the signatory. A digital certificate is like an identification card. The CA verifies the signatory's identity and issues the certificate.

(2) Controls. Digital electronic signatures that use PKI and incorporate digital certificate authentication contain controls that ensure the authenticity of the signature. This technology also ensures the signature is permanently embedded in the document, record, or data in such a way as to render the content unalterable without a new signature.

2.2 ELECTRONIC SIGNATURE PROCESS.

A certificate holder's electronic signature process should describe, contain, or address the following:

a. Uniqueness. An electronic signature is only valid if it is unique to the individual signatory. It should identify a specific individual and be difficult to duplicate.

b. Control. A valid electronic signature must be under the sole control of the signatory and require the signatory to use a unique user name and password to access the system and affix the signature.

c. Notification. The system should notify the signatory that the signature has been affixed.

d. Intent to Sign. The signatory should be prompted before their signature is affixed. The electronic signature block should contain a word or statement of intent that definitively conveys the signatory's intent to affix his or her signature. Examples of statements that do this include, but are not limited to:

• "Signed by,"
• "Certified by,"
• "Instructor's signature/certification,"
• "Signature,"
• "Authorized by,"
• "Signatory,"
• "Authentication,"
• "Acknowledged by,"
• "Acknowledgement," and/or
• "Affirmed by."

e. Deliberate. An individual using an electronic signature should take deliberate and recognizable action to affix their signature. Acceptable deliberate actions for creating an electronic signature include, but are not limited to, the following:

- Using a digital signature;
- Entering a user name and password;
- Swiping a badge; and/or
- Using an electronic stylus.

f. Signature Association. A signature must be attached to, or logically associated with, the record being signed; otherwise, it is not legally significant. There are two aspects to this issue:

(1) It must be clear to the signatory exactly what it is that they are signing. In an electronic environment, the signer must have an opportunity to review the record before signing it, and to clearly understand the parameters of the record they are signing. It is also critical that the signing process be established in a manner to ensure that the signatory's electronic signature is applied only to what they can review.

(2) The electronic form of signature applied by the signer must be linked to the record being signed. Satisfying this requirement requires storing the data constituting the electronic form of signature and doing so in a way that permanently associates it with the electronic record that was signed.

g. Retrievable and Traceable. The user should be able to identify and retrieve the documents to which his or her electronic signature has been applied. An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

h. Undeniable. A valid electronic signature is one that cannot be denied (repudiated) by the signer. An electronic signature process must contain procedures and controls designed to ensure the authenticity of the signature and that the signer cannot deny having affixed the signature to a specific record, document, or body of data.

i. Security Protocols and Prevention of Unauthorized Access and Modification. An electronic signature process must be secure and must prevent unauthorized access to the system

that affixes the signature to the intended documents or records. The process must ensure that only the intended signatory can affix his or her signature and must prevent unauthorized individuals from certifying required documents, such as airworthiness or dispatch releases. The process must prevent modifications to information/data or additional entries to records or documents without requiring a new signature. Additionally, the process must contain restrictions and procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment.

j. Permanent and Unalterable. A valid electronic signature must be a permanent part of the record or document to which it was affixed. The information contained in the record or document must be unalterable without a new signature to validate the alteration.

k. Identification and Authentication. Electronic signature software must have authentication capabilities that can identify a signature as belonging only to a particular signatory. An individual using an electronic signature should be required to use a method of authentication that positively identifies the individual within the electronic signature system.

l. Correctable. An electronic signature process should include a means for a certificate holder to correct records or documents that were electronically signed in error, as well as those documents where a signature is properly affixed but the information or data is in error. An electronic signature should be invalidated any time a superseding entry is made to correct the record or document. The information or signature being corrected should be voided but remain in place. The new information and/or signature should be easily identifiable.

m. Archivable. 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.

n. Control of Private Keys and Access Codes. A digital electronic signature process must ensure the private key or access to the electronic system that affixes the signature is under the sole custody of the signatory at all times.

o. Policies and Procedures. When constructing an electronic signature process, the certificate holder's manual should include the following elements:

(1) Procedures. Procedures should address how the applicable regulatory requirements for their program are met. These procedures should be available to all users of the system.

(2) Description of Electronic Signature Process. A description of the electronic signature process must be included in the certificate holder's manual. The description should explain how electronic signatures will be used and how electronic signatures are applied throughout the certificate holder's operation (e.g., dispatch releases, training records, airworthiness releases, and maintenance actions). For commercial operators operating under Part 9 each electronic signature process must be identified by a revision number and date. For a new unrevised process, a certificate holder may identify the revision number as "0" or "Original." A reference to the process revision number and date, as well as the manual that contains the description of the electronic signature process, will be part of the authorization.

(3) Responsible Personnel. Policies and procedures should identify the certificate holder's personnel who have the authority and overall responsibility for the integrity and security of the

electronic signature process and for controlling access to the computer software/application used in the process. Policies and procedures should also identify the persons with the authority and responsibility for modifying, revising, and monitoring the electronic signature process, as well as ensuring the process is followed by all appropriate personnel.

(4) Identification of Persons Authorized to Use Electronic Signatures. Certificate holders must have a system for identifying who is authorized to use the electronic signature process, for what purposes, and which records.

(5) Description of System Support. Policies and procedures should address system support of any computer hardware or software that is part of the electronic signature process.

(6) Hardware and Software Capabilities. Description(s) of the electronic signature hardware to be used and software capabilities for applications of electronic signatures in the certificate holder's system(s).

(7) Auditing Process. Electronic signature policies and procedures should include an auditing process to ensure all of the requirements for electronic signatures continue to be met. The process should include unauthorized event recognition, which includes actions to be taken by the certificate holder upon discovery of an attempt by an unauthorized individual to use an electronic signature.

(8) Process Changes. A certificate holder's electronic signature process policies and procedures should address how the certificate holder will submit changes to the electronic signature process to the ECAA for acceptance. Commercial operators operating under Part 9 will be required to identify changes to the process by revision number and date. This information will become part of the authorization. For all operations to which this AC applies, revisions to the electronic signature process must be included in the manual or official document containing the electronic signature process description.

(9) Data Backup and Retention. Policy and procedures should address how data backup and retention of data will be accomplished.

(10) Procedures for Computer System Outages and/or Disaster Recovery. Policy and procedures should address computer system outages (failure of hardware, software, application, network, etc.) or disaster recovery.

(11) Training and User Instructions. A certificate holder's policies and procedures should include any training and instructions necessary to ensure authorized users understand how to access and properly apply the electronic signature process. Procedures should describe how users are notified of changes to the electronic signature process.

2.3. ELECTRONIC SIGNATURE AUTHORIZATION.

a. Application Submission. Certificate holders should submit their application to use an electronic signature process to ECAA. The application medium (paper or electronic file) must be acceptable to both the applicant and the ECAA. ECAA will review the application package for accuracy and completeness according to the General Process for Approval or Acceptance of Applications and discuss any deficiencies with the certificate holder. The ECAA may also

notify the certificate holder in writing of any application deficiencies. Before ECAA accepts the application package, the certificate holder will be required to correct all of the deficiencies. A certificate holder's application package for authorization to use electronic signatures must include the following:

(1) Letter of Intent. The application must contain the certificate holder's letter of intent to use electronic signatures.

(a) Estimated Date of Implementation. The letter must include the estimated date on which the certificate holder would like to begin using electronic signatures.

(b) Primary Point of Contact (POC). The letter must include the certificate holder's primary POC for the electronic signature process application.

(2) A Description of the Proposed Electronic Signature Process. The electronic signature process description must address all of the requirements contained in paragraphs 2-1 and 2-2 of this AC.

(3) The Documents and/or Records That Will Contain an Electronic Signature. The application must state specifically which documents or records the certificate holder desires to contain an electronic signature.

(4) Manual Containing the Electronic Signature Process. The certificate holder must include a copy of the manual(s) (or document for operations that do not require a manual) that contains the electronic signature process description.

b. Demonstration of the Process. The ECAA will require a certificate holder to demonstrate the electronic signature process. The items requiring demonstration will typically include at least the following:

(1) Hardware and Software Capabilities. The certificate holder should demonstrate the actual electronic signing of a document.

(**2) Security Protocols and Prevention of Unauthorized Access and Modification.** The certificate holder should demonstrate the following:

(a) How the electronic signature process prevents unauthorized personnel from signing a document or record.

(b) How the process prevents anybody other than the intended signatory to affix his or her signature.

(c) How modifications to a signed document are prevented without a new signature.

(d) How the signature is permanently affixed to the document or record being signed.

(3) Quality Control (QC) Procedures. The certificate holder should demonstrate its QC procedures for ensuring the security and authenticity of electronic signatures.

c. Successful Completion of Application Process for Acceptance and Authorization. When a certificate holder successfully completes the application and demonstration process, the ECAA will accept the electronic signature process and authorize its use by approving the authorization in the company's approved manual.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the electronic signature process, the ECAA will reject the application and provide an explanation to the certificate holder in writing.

Refer to Appendix A for the detailed guidelines (checklist) to facilitate implementation of such system(s).

CHAPTER 3. ELECTRONIC RECORDKEEPING

3.1. ELECTRONIC RECORDS. An electronic record may be a record generated electronically by an electronic transaction, or an electronic image of a paper record. When constructing an electronic recordkeeping system to meet the operational and maintenance requirements in this Advisory Circular, the following information elements shall be considered and addressed in the manuals required by regulations or in the directions for the system. This information shall be made available to each individual responsible for using the system. An electronic record must provide equivalent or better data integrity, accuracy, and accessibility to what would otherwise be provided by a paper record. In general, a record preserves the evidence of an event. It should contain enough information to clearly depict the event that took place. It is the certificate holder's responsibility to address all requirements for their recordkeeping system(s) applicable to their operation(s).

3.2. STANDARDS FOR ELECTRONIC RECORDS.

To be considered complete and valid, an electronic record should contain at least the following information:

- The type of event that took place (e.g., training, maintenance performed, signing of a release, conduct of a flight, etc.);
- For a training event, information that shows compliance with regulatory requirements, such as the name of the course module or subject, the number of hours of instruction, whether the student passed or failed, etc.;
- When the event took place (e.g., the date and time (where appropriate);
- Where the event took place (e.g., the station, training facility, maintenance facility, etc.);
- Who was involved in the event (e.g., crewmember, dispatcher, instructor, mechanic, etc.);
- Aircraft type and registration number for pilot logbook records (when required by regulation);
- Certification, verification, or authentication of the event, such as a signature, where required by regulation; and
- Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (M/M) for maintenance records, such as life-limited parts and time-in-service records.

3.3. ELECTRONIC RECORDKEEPING SYSTEM.

Electronic recordkeeping system(s) should include the following elements:

a. Security.
(1) The system should protect confidential information.
(2) The system must ensure that the information in an electronic record is not altered in an unauthorized way.
(3) The system must provide for secure access and contain safeguards against unauthorized access.
b. Procedures. Electronic recordkeeping system procedures must be incorporated into the certificate holder's manual system. Procedures should include at least the following:
(1) Procedures for Making Required Records Available to ECAA and Accident Investigation Bureau (AIB) Personnel. A certificate holder must provide its records in a format and manner that is acceptable to the requesting Authority. ECAA personnel assigned to a certificate holder with an electronic recordkeeping system may request a certificate holder to provide direct access to the electronic system for the purpose of inspecting regulatory records. In accordance with the relevant Parts of Civil Aviation Rules, each employee of, or person used by, the certificate holder who is responsible for maintaining the certificate holder's regulatory records applicable to the operation of the certificate holder) must make those records available to the Authority personnel.
(2) Quality Control (QC). The system should have procedures for auditing the computer system periodically to ensure the quality, integrity, and accuracy of the system. If workstations are server-based and contain no inherent attributes that enable or disable access, there is no need for each workstation to be audited. (A record of the audit should be completed and retained on file as part of the certificate holder's record retention requirements. This audit may be a computer program that automatically audits itself.)
(3) Maintenance Support and Backup Measures. The system should include procedures for maintenance and support that include provisions for electronic system (computer hardware, software, application network, etc.) outages and protect against the loss of record data. The system should also include backup measures to maintain and provide access to records in the event of a system failure. The backup system may be a separate electronic system, a backup server, or backup drive. Backup can also include media such as print or CD-ROM, external drive, or other media acceptable to the ECAA.
(4) Record Transfer. Procedures should ensure that records transferred with an aircraft (either electronic or on paper) meet regulatory requirements.
(5) Persons with Authorized Access. The system procedures should contain guidelines for authorized representatives of the certificate holder to use electronic recordkeeping and to have access to the appropriate records (each representative with authorization to make entries shall be issued a unique individual access code and password in order to validate the entry). In particular, procedures should specifically address instructor, evaluator, and supervisor access to the system.
(6) Electronic Authentication, Signature, Validation, or Endorsement. Most records required by Civil Aviation Regulations require some kind of validation, such as a signature, certification, endorsement, or authentication. This validation must be a permanent part of any

electronic record. Any electronic form of validation must meet the legal requirements of electronic signing as outlined in this AC.

(7) Training and User Instructions. Each electronic recordkeeping system should contain training and user instructions for the persons responsible for entering, maintaining, and retrieving data from the system. Training should include security awareness and system integrity, as well as procedures that are necessary to authorize access to the electronic recordkeeping system. User instructions should include those for ECAA personnel who are provided direct access to the system.

(8) Transferring Data. Technological advances may make it desirable or necessary for a certificate holder to update its electronic recordkeeping system or transfer data to a new system. The certificate holder must have policies and procedures that ensure the continued integrity of record data when a certificate holder moves records from one system to another. This could entail running redundant systems for a brief period of time.

(9) Continuity of Data between Legacy and Electronic Systems. The system should have a method of ensuring continuity of data during transition from a legacy (hardcopy) system to an electronic system.

(10) Continuity of Records for Maintenance Providers. Procedures should ensure continuity with maintenance providers. Certificate holders must ensure there is continuity between their program(s) and their maintenance provider's programs. This is necessary to ensure the quality and integrity of each record that is maintained via the electronic recordkeeping system.

c. Responsible Personnel. Policies and procedures should identify the certificate holder's personnel who have the authority and overall responsibility for the integrity and security of the electronic recordkeeping system and who are responsible for controlling access to the system. Policies and procedures should also identify the persons with the authority and responsibility for modifying the electronic recordkeeping system, as well as those who are responsible for entering data into the system.

d. Description of Electronic Recordkeeping System(s). There may be more than one system required to maintain various kinds of records. Each electronic recordkeeping system used by the certificate holder must be described in its manual. Each electronic recordkeeping system description should address the information and elements contained in paragraphs 3-1, 3-2, and 3-3 of this AC, as well as the following:

(1) Description of electronic recordkeeping system(s) to include system facilities, hardware, and software.

(2) Identification of records that will be maintained in the electronic system(s).

(3) Identification of which electronic records on which the certificate holder will use an authorized electronic signature process.

e. Changes to the Electronic Recordkeeping System. A certificate holder's policies and procedures should include details of when revisions to the electronic recordkeeping system will be submitted for approval or acceptance (depending on the regulatory requirement) prior to implementation. This includes new versions of system software. For all operations to which this

AC applies, changes to the electronic recordkeeping system must be included in the manual or official document containing the electronic recordkeeping system description.

f. Audit Procedures. The certificate holder must have auditing procedures that ensure the quality and integrity of each record maintained in the system and that all of the requirements of the electronic recordkeeping system continue to be met. Procedures should include unauthorized event recognition, which includes actions to be taken by the certificate holder upon discovery of an attempt by an unauthorized individual to access and/or make entries into the electronic recordkeeping system.

3.4. ELECTRONIC RECORDKEEPING AUTHORIZATION.

a. Application. Certificate holders should submit their application for an electronic recordkeeping process to ECAA. The application medium (paper or electronic file) must be acceptable to both the applicant and the ECAA. The ECAA will review the application package according to the General Process for Approval or Acceptance of Air Operator Applications. The ECAA will review the application package for accuracy and completeness and discuss any deficiencies with the certificate holder. The ECAA may also notify the certificate holder in writing of any application deficiencies. Before ECAA accepts the application package, the certificate holder will be required to correct all of the deficiencies. A certificate holder's application package for authorization to use an electronic record keeping system must include the following:

(1) Letter of Intent. The application must contain the certificate holder's letter of intent to use an electronic recordkeeping system.

(a) The Name of the Electronic System(s). The letter must include the kinds of records along with the name of the electronic system to be used to maintain the records. There may be more than one system required to maintain various kinds of records.

(b) Estimated Date of Implementation. The letter must include the estimated date on which the certificate holder would like to implement the electronic recordkeeping system.

(c) Primary Point of Contact (POC). The letter must include the certificate holder's primary POC for the electronic recordkeeping system application process.

(2) A Description of the Proposed Electronic Recordkeeping System(s). The electronic recordkeeping system description must address all of the requirements contained in paragraphs 3-1, 3-2, and 3-3 of this AC, and include a description of the system facilities, hardware, and software. Software version numbers must be included.

(3) The Records that will be maintained in the System. The certificate holder must state specifically which records the certificate holder intends to maintain and access via the electronic recordkeeping system. The application should include a sample of each record type.

(4) The Data Backup. The application must describe the details of the certificate holder's data backup system.

(5) Access and Security Procedures. The application must include information regarding access and security procedures.

(6) Electronic Signature Processes. The application must include a description of any electronic signature process associated with each electronic record category.

b. Demonstration of the System. The ECAA will require a certificate holder to demonstrate the electronic record keeping system. The items requiring demonstration will typically include at least the following:

(1) User Access. The certificate holder should demonstrate how to securely access the system.

(2) Security Protocols and Prevention of Unauthorized Access and Record Modification. The certificate holder should demonstrate how the system prevents unauthorized access or modifications to the records maintained on the system.

(3) Record Entry. The certificate holder should demonstrate how a record is entered into the system.

(4) QC Procedures. The certificate holder should demonstrate the procedures for ensuring the quality and integrity of each record maintained on the system.

c. Successful Completion of Application Process for Approval or Acceptance and Authorization. When the certificate holder successfully completes the application and demonstration process, the ECAA will approve the electronic recordkeeping system and authorize its use.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the electronic recordkeeping process, the ECAA will reject the application and provide an explanation to the certificate holder in writing.

Refer to **Appendix A** for the detailed guidelines (checklist) to facilitate implementation of such systems.

CHAPTER 4. ELECTRONIC MANUAL SYSTEMS

4.1. ELECTRONIC MANUALS. Like printed manuals, electronic manuals must provide instructions and information necessary to allow personnel concerned to perform their duties and responsibilities with a high degree of safety. The electronic manuals offer improved data accessibility and speedy distribution over paper-based information storage systems, however, an electronic manual must provide equivalent or better data integrity, accuracy, and accessibility to what would otherwise be provided by a printed manual. The content of each electronic manual must be clearly identifiable and viewable by the user and must correlate and be comparable to what would be available in a printed version of the manual. An electronic manual should contain elements that generally comprise a printed manual. These elements typically include:

- The manual title;
- Revision control pages or sections from which the user can readily determine whether the manual is current;
- List of effective pages;
- Indication of ECAA approval (e.g., signature or stamp) for those manuals or manual sections that require ECAA approval;

- Chapter numbers;
- Chapter headings;
- Section numbers;
- Topic headings;
- Page numbers;
- Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (M/M) (when applicable for minimum equipment list (MEL) and maintenance purposes); and
- The person with the authority and responsibility for manual content.

4.2. ELECTRONIC MANUAL SYSTEM.

An electronic system for delivering manual content must comply with regulatory requirements for currency, availability, and distribution to the appropriate personnel. A certificate holder's electronic manual system must address any Civil Aviation Regulation requirements for "must" or "should" that apply to their operation(s) into their electronic manual system. An electronic manual system should describe/address:

a. Currency. Each certificate holder's electronic manual system method of keeping each manual current.

b. Access, Availability, and Distribution. Each electronic manual system should provide distribution and/or access to manual(s) by the appropriate personnel, in a form and method acceptable to the Administrator.

c. MEL Direct Access Requirement. As required by Part 9 air operators who conduct operations under Part 9 must provide the flight crew members, maintenance personnel and persons assigned operational control functions during the performance of their duties with direct access to the MEL through printed or other means approved by the Administrator. An Electronic Flight Bag (EFB) is an example of other means that may be approved by the ECAA.

d. ECAA and Accident Investigation Bureau (AIB) Access. The ECAA requires certificate holders to provide access to the electronic manual system to the appropriate ECAA representatives on their official duty. When providing such access, a certificate holder should provide the ECAA's representatives with instructions on how to access the system. Certificate holders must provide any requested information to the Accident Investigation Bureau (AIB) in the event of an accident or incident. When a certificate holder is required to provide manuals or manual information to the ECAA or Accident Investigation Bureau (AIB), it should be provided in the desired format of the requesting Authority.

e. Responsible Personnel. The system description should include the certificate holder's personnel who have the authority and responsibility for maintaining the system, implementing, modifying, revising, and monitoring the electronic manual software and ensuring the overall integrity of the content of manuals that are part of the system.

f. Prevention of Unauthorized Access and Data Corruption. Manual system computer hardware and software must prevent unauthorized access and/or modification to electronic manual content.

g. Storage and Retrieval. The computer hardware and software system must store and retrieve the manual's content under conditions of normal operation and use. The system must not permit unauthorized modification of the data it contains.

h. Functionality. Users should be able to easily access, navigate, and retrieve manual content via computer or comparable device. Manual users should be able to print any information contained in an electronic manual.

i. Revision Control. A certificate holder's electronic manuals should be easy to revise. The electronic manual system should include revision control procedures for making revisions (incremental, temporary, and scheduled) in a timely manner. Procedures should include the accomplishment of revisions by personnel to whom manuals are issued. The revision control procedures should address at least the following:

(1) Communication of Revision Information. Procedures should include the method of communicating revision information, similar to what would be provided for a paper manual revision. Revision information should provide the revision content, effective date, and any instructions required for ensuring the revision is uploaded or incorporated into the electronic manual. Revision information should allow the user the ability to compare the current revision to the previous version, or it should explain the effect of the change. The revision system should make changes under the current revision readily apparent. An example of this would be change bars. An electronic manual should contain a revision control page or section from which the user can readily determine whether the manual is current.

(2) Revision Status of Each Manual Page. Each page of a manual should contain the date of the latest revision for that particular page. If an electronic manual is distributed via a device that displays the manual in a continuous flow format, as opposed to page-by-page, then each section or block of information displayed on the device must contain the date of the latest revision.

(3) Date and Time Stamp of Printed Information. When information from an electronic manual is printed, there should be a means to identify the date and time of printing. This ensures the currency of information by allowing the manual user to compare the date of the printed information with the date of the information contained in the electronic manual system. Printed information that has the same date, but differs from the information contained in the electronic manual, would indicate that the manual content was printed before the manual was updated later that day.

(4) User Responsibility for Current Information. Users of electronic manuals who need or elect to print material (data information, instructions, procedures, etc.) from the electronic manual must ensure the printed information is the most current available prior to use. Users should discard printed manual information after using it to ensure printed information does not become outdated.

(5) Distribution and Submission of Manual Revisions to the ECAA.

(a) Revision control procedures should include the certificate holder's method of distributing paper copy and electronic revisions to the ECAA.
(b) When a particular manual requires ECAA approval, the certificate holder's procedures should explain how the certificate holder will submit an electronic revision to the ECAA for approval or acceptance of the revision content.

j. Special Considerations in Displaying Information. Information retrieved from an electronic manual could be displayed in a format that differs from what would appear on paper. The display format could even vary by user. For example, the display of manual content could be different for pilots on the flight deck of an aircraft versus what is displayed to ground personnel at a computer workstation. This could occur for reasons such as screen resolution, software application, or authorized display device. Information displayed on any authorized device on the flight deck must correlate to information displayed at an authorized computer workstation or authorized portable device. Additionally, any information displayed should be easily traceable and comparable to the source document. The most important point is that the electronic manual content must remain the same, regardless of the display format or device. Any displayed manual information must be identical in content for all users.

k. Data Archiving. An electronic manual system should have a method of archiving technical and procedural data superseded by revision. A certificate holder should archive earlier versions of manuals to provide for future needs to duplicate, regenerate, or reconstruct instructions.
(1) The Importance of Historical Data. Archived historical data is particularly important for the following reasons:
(a) To trace aircraft repair information or reconstructing maintenance instructions.
(b) To evaluate normal and abnormal flight deck (cockpit) checklist procedures.
(c) For training purposes.
(d) For investigation purposes in the event of an accident, incident, or occurrence.
(2) Preservation of Archived Data. An electronic manual system must have procedures to ensure the integrity of the archived technical and procedural data. These procedures should include at least:
(a) A method of ensuring that no unauthorized changes can be made.
(b) A method or medium that minimizes the deterioration of data.
(c) A method to protect the archived data against hazards and natural disasters.

l. Transferring Data to Another System. Technological hardware or software advances may make it desirable and/or necessary for a certificate holder to update its electronic manual system. When transferring manual data from one electronic system or application to another, certificate holders should ensure that data integrity is maintained during transfer. This includes ensuring that archived information remains intact. This could entail running redundant systems for a brief period of time.

m. Backup Method. A certificate holder that uses an electronic manual system must have a backup method of maintaining, distributing, or otherwise providing access to manuals, in case of system hardware or software failure. The backup method may be a separate electronic

system; a backup server to the authorized system; the use of backup media such as print or CD-ROM; or other method acceptable to the ECAA.

n. System Maintenance and Support. Each certificate holder's electronic manual system should include maintenance and support function that identifies hardware and software failures within the system. System maintenance and support should include provisions for system outages and for switching over to the backup method described in subparagraph 4.2 (m) above.

o. Master Manual for Parts. An electronic manual system used in operations under Part 9 must include a master manual that describes the electronic manual system and lists each manual maintained and distributed via the system. The master manual must include at least the following:

(1) Description of the Electronic Manual System. The electronic manual system description should include the methods for distribution and/or access to manual(s) (including manual revisions and replacements) by the appropriate personnel.

(2) Delivery Media. An electronic manual system description must include an explanation of the media by which the manuals will be distributed to required personnel.

(3) Personnel with Authority and Responsibility. The master manual must list the certificate holder's personnel who have the overall authority and responsibility for maintaining the electronic manual system.

(4) Listing of Manuals—Certificate Holders with Large and Complex Manual Systems. For a certificate holder with a large and complex manual system that contains numerous manuals, it is acceptable to list the kinds of manuals, instead of listing each manual, provided all of the particular kinds of manuals are maintained and distributed via the electronic manual system. For example, list "All Ground Operations Manuals," "All Maintenance Manuals," or "All Training Program Manuals."

p. Description of the Electronic Manual. For electronic manuals used in Part 6 a description of how each electronic manual is displayed, maintained, revised, and distributed should be included in the certificate holder's manual system. The description must also include an explanation of the media by which manuals will be distributed to required personnel.

q. Electronic Manual System Changes. Policy and procedures should address how the certificate holder will submit changes to the electronic manual system to the ECAA for approval. For certificate holders operating under Parts 3, 6, 9 changes to the electronic manual system must be documented through revision to the master manual containing the electronic manual system description.

r. User Instructions and Training. Each certificate holder must provide instructions and training to users of the electronic manual system. The scope and complexity of the training may vary depending on an individual's duties and responsibilities. Training should include security awareness and computer system (hardware, software, application, network, etc.) integrity.

4.3. ELECTRONIC MANUAL AUTHORIZATION.

a. Application. Certificate holders should submit their application for an electronic manual system to ECAA. The application medium (paper or electronic file) must be acceptable to both the applicant and the ECAA. ECAA will review the application package for accuracy and completeness according to the General Process for Approval or Acceptance of Applications and discuss any deficiencies with the certificate holder. The ECAA may also notify the certificate holder in writing of any application deficiencies. Before ECAA accepts the application package, the certificate holder will be required to correct all of the deficiencies. A certificate holder's application package for authorization to use an electronic manual or manual system must include the following:

(1) Letter of Intent. The application must contain the certificate holder's letter of intent to use an electronic manual system.

(a) Estimated Date of Implementation. The letter must include the estimated date on which the certificate holder would like to implement the electronic manual system.

(b) Primary Point of Contact (POC). The letter must include the certificate holder's primary POC for the electronic manual system application process.

(2) Master Manual for Commercial Air Operators. An application to use an electronic manual system for operations conducted under Part 9 must include a copy of the proposed master manual as described in subparagraph 4.2(o) of this AC.

(3) A Description of the Proposed Electronic Manual for Approved Maintenance Organizations. An application to use an electronic manual for Approved Maintenance Organizations under Part 6 must include a description of the electronic manual as described in paragraph 4.2 (p) of this AC.

(4) Manuals Included in the System. The application must state specifically which manuals the certificate holder intends to maintain and distribute electronically:

- Flight Operations Manuals (FOM) by title;
- Ground operations manuals by title;
- Maintenance manuals by title;
- Training program manuals by title;
- Electronic MELs;
- General policy manuals by title; and
- User manuals (e.g., flight planning system and other hardware/software applications) by title.

(5) Distribution to the ECAA. The certificate holder must provide a copy of the electronic manuals to ECAA and provide an explanation of how revisions and future electronic manuals will be distributed to the ECAA.

(6) Electronic Access to an MEL. Operations conducted under Part 9 require a certificate holder to have ECAA approval to provide access to an MEL. Certificate holders desiring to

provide electronic access to an MEL must specify that in the application and include details on how electronic access will be provided.

b. Demonstration of the System. The ECAA will require a certificate holder to demonstrate the electronic manual system. The items requiring demonstration will typically include at least the following:

(1) Hardware and Software Capabilities. The certificate holder should demonstrate how to use the hardware and software by performing simple tasks within the system.

(2) Distribution and Availability. The certificate holder should demonstrate how the manuals will be distributed or made available (depending upon the regulatory requirement) to required personnel electronically.

(3) Information Access Capabilities. The certificate holder should demonstrate how to access manual content via the electronic system.

(4) Prevention of Unauthorized Modification. The certificate holder should demonstrate how the system prevents unauthorized modifications to manual content.

(5) Revision Capabilities. The certificate holder should demonstrate how revisions are posted to electronic manuals.

c. Successful Completion of Application for Approval or Acceptance and Authorization. When a certificate holder successfully completes the approval (applicable only to electronic access to an MEL) or acceptance process, the ECAA will authorize the electronic manual system by signing and issuing authority in the approved manual.

d. Unsuccessful Application. If the certificate holder fails to submit an acceptable application or fails to successfully demonstrate the manual system process, ECAA will reject the application and provide an explanation to the certificate holder in writing.

Refer to **Appendix A** for the detailed guidelines (checklist) to facilitate implementation of such systems.

APPENDIX "A"

Compliance Checklist for Electronic Signatures, Electronic Records, and Electronic Manual Systems.

No.	CONTROL STEPS	CHECKS
A. SECURE ELECTRONIC SIGNATURES		
1	Determine whether the security procedure is reasonable based on: (a) nature of the transaction; (b) sophistication of the parties; (c) volume of similar transactions engaged in by either or all parties; (d) availability of alternatives (e) cost of alternative procedures; and (f) Procedures in general use for similar types of transactions.	Assess whether the means of identification and authentication (e.g. User-ID and password, onetime or dynamic password, biometrics, digital certificate) used are adequate, suitable and effective for the system.
2	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables an electronic signature to provide a unique identification with reasonable certainty. Through control and archives, the system should be capable of determining if the signature is genuine and if the individual is authorized to participate. This capability should be an integral part of the system.	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.
3	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables an electronic signature to prevent a signatory from denying that he or she affixed a signature to specific record, record entry or document.	Check that the system's security features can adequately prevent others from duplicating the signatures or alter signed documents. This is to ensure nonrepudiation that the signature was indeed made by the signatory.
4	Verify whether the electronic system that produces signatures is able to restrict individuals from affixing another individual's signature to a record, record entry or document.	Check that the system is able to prevent an unauthorized individual from certifying required documents, such as certificate of release to service.
5	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables an electronic signature to be created in a manner or using a means under the sole control of the person using it.	Check that the system has acceptable and deliberate actions for creating electronic signature which includes, but not limited to,

		badge swipes, signing with stylus, typing specific keystrokes or using a digital signature.
6	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables an electronic signature to be linked to the electronic record to which it relates in a manner such that if the record was changed the electronic signature would be invalidated.	Check that the system has a means to invalidate signed records once the electronic signature has been tempered with.
7	Verify that a means of safely archiving electronically-signed documents is part of any electronic signature computer software.	Check that the electronic records are archived completely and accurately.
8	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables an electronic signature to provide positive traceability to the individual who signed a record, record entry or any other document.	Check that there are adequate audit logs to track all changes made to the electronic records and these logs are periodically reviewed.
9	Verify whether the application of a specified security procedure or a commercial reasonable security procedure 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.	Check and ascertain that the process for revocation of the user's electronic signature is adequate, effective and properly logged.
10	Verify whether specified security procedure or a commercial reasonable security procedure is established to allow 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.	Check that the entry should be voided but remain in place. Reference to a new entry should be made and electronically signed and dated.
11	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.	Check that the system is able to ensure that the identified material is, in fact, what is being signed for after affixing the signature. 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 since electronic documents may not position a signature in the same way as handwritten documents. Acceptable methods of marking the affected areas

		include, but are not limited to, highlighting, contrast inversion, or the use of borders or flashing characters. The system should also notify the signatory that the signature has been affixed.
B. SECURE ELECTRONIC RECORDS		
12	Verify whether the application of a specified security procedure or a commercial reasonable security procedure enables the information in the electronic recordkeeping system to be kept confidential.	Check and verify that the system has reasonable security measures to ensure the confidentiality of the electronic records. An electronic record may be a record generated electronically by an electronic transaction, or an electronic image of a paper record.
13	Verify whether the application of a specified security procedure or a commercial reasonable security procedure ensures that the information in the electronic recordkeeping system is not altered in an unauthorized way.	Check and verify that the system has reasonable security measures to ensure the integrity of the electronic records. Maintenance of the integrity of the information could be accomplished by having a record of transactions, including records of entries created and altered which identifies the person responsible for the transaction by name, and the date and time of the transaction. Corrected errors or alterations to the records need to be identified and the reason for the correction included and reviewed.
14	Verify that the electronic system is capable of reconstructing the record if there is a requirement to retain a signature, document or information.	Check that the requirement to produce a document is not nullified by the destruction of a primary data storage, such as RAM and cache.
15	Verify whether the application of a specified security procedure or a commercial reasonable security procedure ensures that when a document is changed, the changes can be tracked and all users can access the most updated version.	Check that there is version tracking for the electronic records.
16	Verify whether there are procedures for making the	This procedure and computer

	required records available to ECAA officers and the Accident Investigation Bureau (AIB) of Ministry of Transport (MoT).	system should be capable of making paper and soft copies of the viewed information at the request of ECAA and the AIB of MoT.
17	Verify whether there are procedures for auditing the computer system annually to ensure the confidentiality, integrity and availability of the system. The key components of the system (e.g. servers, perimeter network devices, security components, interfaces) should be audited. For the non-key components, it is acceptable to do a sampling and audit one of each type. The remediation for the sampled component should then be propagated to the rest of the non-sampled ones.	The applicant shall submit credentials of the auditor when seeking ECAA' acceptance of the electronic system.
18	Verify whether the application of a specified security procedure or a commercial reasonable security procedure describes how the operator will ensure that the computerized records are transmitted in accordance with the appropriate regulatory requirements to customers or to another operator in a format acceptable to them.	Check whether records comply with record keeping requirements prescribed in relevant Parts of ECARs.
19	Verify whether the application of a specified security procedure or a commercial reasonable security procedure 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.	
20	Verify whether there are guidelines for authorized representatives of the owner/operator to use electronic signatures and to have access to the appropriate records.	
21	Verify whether there are training procedure and requirements necessary to authorize access to the computer hardware and software system. Users of the system shall also be trained on its proper usage and regularly briefed on ICT security.	
C. ELECTRONIC MANUALS/DOCUMENTS		
22	An electronic manual shall address the following operational and maintenance requirements: **<u>Storage and Retrieval</u>** Computer hardware and software system should store and retrieve the technical data under conditions of normal operation and use. The system should not permit unauthorized modification of the data it contains.	

	Maintenance and Support Maintenance and support for the system, including provisions for outages and necessary alternative retrieval services may be provided by sources independent of the approval holder or operator. However, the approval holder or operator is still responsible for compliance with all regulatory requirements and cannot be delegated. **Access to Document** Procedures for distributing the documents/technical data may be similar to procedures distributing information contained in hardcopies. Approval holders or operators may use their current document distribution system to distribute electronic documents. **Revisions to Document** Procedures to verify that revisions (i.e., incremental, temporary or scheduled revisions) to the technical data contained in the documents are current and complete. In addition, revisions should be approved by the appropriate authority before distribution. **Revision Control Procedures** (a) Procedures should be established to audit the revision process to ensure contents of the electronic system are current and complete. (b) Approval holders or operators may issue transmittal letter or release notes to specify the current revision number and date for each revision. A user can inspect and review these documents to determine data currency. (c) Procedures should be established to ensure the currency of the technical data. They should ensure that all electronic storage media contain the current revision and associated revision dates. (d) Users of information or printed data from electronic document systems should ensure the information of printed data is from the most current document. **Data Content and Forms of Display** Computer-displayed information shall contain the following: (a) The document title (b) Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model	

	(c) Effective date of the data (d) Revision simultaneously displayed with the technical data **Page Numbers and Revision Data** Therefore approval holders and operators should ensure information displayed or printed can be traced to the correct revision level of the document. Means of referencing the section or page of the document from which data was obtained should be provided. An acceptable method of updating the document is the provision of a table of revisions to identify the pages to which the revision applies (i.e. List of Effective Pages).	
23	Verify whether there are training programs provided to employees who use the electronic document. Training shall include security awareness and procedures for the system.	Acceptable methods of providing this training may include, but not limited to, classroom instruction, online or system tutorials. User guides and simulated problem-solving exercises.
24	Verify procedures to archive earlier versions of documents to provide for future needs to duplicate, regenerate, or reconstruct maintenance instructions. The archived materials should be obtained from the original source of the data. The procedures should include the following: (a) Ensuring no unauthorized changes can be made (b) Selecting storage mediums that minimize regeneration of errors or deterioration (c) Duplicate archived technical data at a frequency compatible with the storage life of the medium (before the storage medium deterioration) (d) Storing duplicate copies in physically separate archives to minimize the risk of data loss in the event of a fire or natural disaster (e) Future systems should be able to retrieve archived technical data. Otherwise, the old system shall be maintained to ensure data availability.	
25	Verify whether there are procedures to ensure capability of making paper copies of the viewed information at the request of ECAA and the AIB of MoT.	This procedure and computer system should be capable of making paper and soft copies of the viewed information at the request of ECAA and the AIB of MoT.

Attachment 1. SAMPLE LETTER OF INTENT [Requester Letterhead]

To: Ethiopian Civil Aviation Authority
From: [Requester]
Date: [Date]

Subject: Use of Electronic System – (Signatures/Recordkeeping/Manuals)

This letter is to inform you that [requester] intends to use an electronic (signatures and/or recordkeeping and/or manual) system for [describe what the system will be used for]. This system has been established using the guidelines outlined in ECAA Advisory Circular (AC) ECAA-AC-GEN005 (as amended).

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

Sincerely,

[Requester]