सत्यमेव जयते
GOVERNMENT OF INDIA
**DIRECTORATE GENERAL OF CIVIL AVIATION**

# AAC NO 4 OF 2023
# Date: 28th December 2023

# AIRWORTHINESS ADVISORY CIRCULAR

**File No. DGCA-25012(07)/10/2023-AW**

**Subject: GUIDANCE FOR ORGANIZATIONS IMPLEMENTING ELECTRONIC SIGNATURES, ELECTRONIC RECORD-KEEPING AND MANUALS.**

## 1. INTRODUCTION:

### A. REASON:

This Advisory Circular (AC) is issued to provide guidance and information on the use of electronic signatures, electronic recordkeeping, electronic documents, as an alternative to paper-based systems, with regard to Organizations seeking to develop and implement Electronic Signature and record-keeping system. It contains information about standards, practices and procedures acceptable to DGCA.

### B. APPLICABILITY:

Organizations highlighted in **Paragraph C** and limited to the scope shown intending to implement Electronic Signature, Records/Documents are responsible for compliance with all regulatory requirements and this responsibility cannot be delegated.

The DGCA supports the use of electronic systems such as electronic signatures, electronic recordkeeping and electronic documents to enable Organizations to develop & implement electronic signatures, records & documents in the aircraft maintenance and production environment. The intent of this AC is to provide guidance with regard to:

1. Electronic Signature
2. Electronic Records System

3. Electronic Documents/Manuals
4. Archiving And Transferability
5. Security And Integrity
6. Organisational Requirements
7. Standards & Technical Specifications
8. Other Forms Of Record Keeping

**Note:** *An Electronic Record or Document is defined as a record or document that is created, stored, generated, copied, sent, communicated or received by electronic means, on a tangible medium or any other electronic medium and is retrievable in perceivable form.*

## C. DGCA REGULATORY REFERENCES

### 1. CAR 21 – Certification Procedures for aircraft and related products and parts

(i) SUBPART G - PRODUCTION ORGANISATION APPROVAL
AMC No. 1 to 21.163(c) - Computer generated signature and electronic exchange of the CA Form 1

### 2. CAR-M CONTINUING AIRWORTHINESS RERQUIREMENTS

(i) SUBPART H - CERTIFICATE OF RELEASE TO SERVICE — AMC M.A. 801(f) Aircraft certificate of release to service
(ii) AMC to Appendix II to CAR-M Use of the CA Form 1 for maintenance (2) Electronic signature and electronic exchange of the CA Form 1

### 3. CAR-145 APPROVED MAINTENANCE ORGANISATIONS

(i) AMC CAR 145.50(b) – Certificate of Maintenance. (as amended)
(ii) APPENDIX I to CAR-145 - AUTHORISED RELEASE CERTIFICATE - AW FORM 1 (Authorised Release Certificate - AW Form 1 – Refer CAR M Appendix II)

### 4. OPERATIONS REGULATIONS

(i) CAR Section 8, Series ‘S’, Part VIII
(ii) CAR Section 8, Series ‘O’, Part II
(iii) CAP 8600

## 2. DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE:

2.1 The Information Technology Act, 2000 provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies.

Digital/Electronic Signature for maintenance, storage, security and authentication

of any information and electronic records, organization shall comply with the provisions of The Information Technology Act. 2000 and its amendment thereof and related rules and notifications issued by the Government under the provision of The Information Technology Act.

2.2 Section 2 of the Information Technology Act defines Electronic Signature and Digital Signature as:

"Digital signature" means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of Section 3 of the Information Technology Act 2000.

"Electronic signature" means authentication of any electronic record by a subscriber by means of the electronic technique specified in the Second Schedule of the Information Technology Act 2000 and includes digital signature.

***Note:*** *The use of the wording "electronic signature" is intended here to capture broad and diverse categories of solutions which, although may be differently identified in the expert field of digital security in accordance with their technological features and capabilities, are all in compliance with provisions 2.5, 2.6 and 2.7 below.*

2.3 The electronic signature is the online equivalent of a handwritten signature. It electronically identifies and authenticates an individual entering, verifying, or auditing computer-based records. The electronic signature should provide a secure authentication of the signatory and should be linked to the data for which the signature was created in such a way that any subsequent change of the data is detectable.

2.4 Electronic recordkeeping systems may be used to generate aircraft operational/ flight/ maintenance records (e.g., maintenance task cards, aircraft maintenance records, airworthiness releases and flight test reports, Journey Log, Mass & Balance) for which there is a need to be able to properly authenticate the user with an electronic signature.

2.5 There are several attributes that an electronic signature should possess:

| Attributes | Description |
|---|---|
| ***Uniqueness*** | ▪ A feature by which the electronic signature should identify a specific individual with reasonable certainty and only that individual, and should be difficult to duplicate.<br>▪ 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.<br>▪ Systems using PIN or passwords could also be an acceptable method of ensuring uniqueness.<br>▪ A computer entry used as a signature should have restricted access that is limited by an authentication code that may be changed periodically or based on procedures established by the organization.<br>▪ Additionally, a system could use physical characteristics, such as a fingerprint, handprint, or voice pattern, as a method of identification and authorization. |
| ***Significance*** | ▪ A feature by which an individual using an electronic signature should take deliberate and recognizable action to affix his or her signature.<br>▪ It provides evidence that an individual agrees with a statement. |
| ***Scope*** | ▪ A feature by which 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 a document.<br>▪ The electronic record should accurately reflect the information being affirmed by signatory and the signatory should be fully aware of what he or she is signing. |
| ***Security*** | ▪ A feature by which an electronic system that produces signatures should restrict other individuals from affixing another individual's signature to a record, record entry, document, or alter the content without trace.<br>▪ To this effect, a corresponding policy and management structure should support the computer hardware and software that delivers the information.<br>▪ The system shall be able to prevent an unauthorized individual from certifying required documents, such as certificate of release to service and prohibit the use of an individual's electronic signature when the individual leaves or terminates employment. |
| ***Non-repudiation*** | ▪ A feature by which an electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. |
| ***Traceability***, | ▪ Which is the feature by which an electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document. |

2.6 The electronic signature solution adopted should adhere to validated requirements and industry standards regarding: the strength of the user/system identification credential employed in creating signatures, the proof-of-possession algorithm for identification credentials, the cryptographic algorithm for protection of data and alternatives that may provide similar protection if the previously enumerated are deemed impractical.

2.7 The electronic signature solution is essentially linked in most cases to the date and time information regarding the moment in which they were created, modified, signed-off. Such information should be appropriately addressed by the time stamping capability of the electronic record keeping system.

2.8 Secure electronic signature: An electronic signature shall be deemed to be a secure Electronic signature if–

(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

## 3. AUTHENTICATION OF ELECTRONIC RECORDS via DIGITAL SIGNATURE AND ELECTRONIC SIGNATURE:

3.1 Section 3 and Section 3A of the Information Technology Act, 2000 provide provisions for the authentication of electronic records and Section 5 gives the legal recognition of electronic signatures.

(1) Subject to the provisions of Section 3 of the Information Technology Act 2000, any subscriber may authenticate an electronic record by affixing his digital signature.
(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

Note: *"hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "hash result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible–*

*(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;*
*(b) that two electronic records can produce the same hash result using the algorithm.*

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

3.2 Electronic signature. –

(1) Notwithstanding anything contained in Para 3.1 above, but subject to the provisions of sub-para (2) of 3.1, a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which–

(a) Is considered reliable; and
(b) May be specified in the Second Schedule of the Information Technology Act, 2000.

3.3 For the purposes of para 3.2, any electronic signature or electronic authentication technique shall be considered reliable if-

(a) The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and of no other person;
(b) The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
(c) Any alteration to the electronic signature made after affixing such signature is detectable
(d) Any alteration to the information made after its authentication by electronic signature is detectable; and
(e) It fulfills such other conditions which may be prescribed in the Information Technology Act, 2000.

3.4 For the authentication of digital signature and electronic signature, rules and regulations issued under Information Technology Act, 2000 (such as Electronic Signature or Electronic Authentication Technique and Procedure (Amendment) Rules, 2015 ; Digital Signature (End Entity ) rules 2015 as well as the notification and guidelines issued by the controller of certifying authorities (CCA) may be adhered to.

## 4. ELECTRONIC RECORDS SYSTEM :

4.1 Acceptable Electronic Recordkeeping System

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 AC, the following information elements should be considered and addressed in the regulatory required manual or in the directions for the system. This information should be made available to each individual responsible for using the system. Refer to **Appendix A** for the checklist to facilitate the implementation of such systems.

4.2 Attributes of an Acceptable Electronic Record keeping System

| Attributes | Description | Functionality / Remarks |
|---|---|---|
| Security | The electronic recording system is capable of protecting information confidentiality | 1. The system is capable of ensuring that the information in the recordkeeping can be kept confidential.<br>2. Identification and authentication procedures can be implemented to enhance security.<br>3. The system is capable of ensuring that theinformation is not altered in an |

| Attributes | Description | Functionality / Remarks |
|---|---|---|
| | | unauthorized way. |
| Integrity | Changes to the records are tracked and verified. All authorised user are able to access the most updated version. | 1. The system is capable of reconstructing the record if there is a requirement to retain a signature, document or information.<br>2. 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.<br>3. A mechanism for version control to ensure current version is readily accessible in respective platforms. |
| Archiving | The electronic recording system is backed up routinely. | 1. The backup system should be robust and reliable.<br>2. There should be a periodic backup schedule that backups the records at pre-determined frequencies to ensure minimum data-loss.<br>3. The recovery of data from the backup should also be demonstrated. |

Where IT systems are used to retain documents and data, this should include unrestricted access for auditing and the capability of the Organization to provide paper copies of needed records, if required by the DGCA. Procedures should be in place to ensure the capability of making paper copies. For example, Print out of electronic records should have a watermark displayed on the page background stating "PRINTED FROM ELECTRONIC FILE". The watermark is an example and is not the only means.

## 5. ELECTRONIC DOCUMENTS/ MANUALS:

### 5.1 General

These electronic formats offer improved data accessibility, quality control, and speed distribution over paper-based information storage systems that result in enhanced safety. Electronic manual computer hardware and software systems should deliver the same, or better, accuracy and integrity maintained by paper-based systems. Refer to **Appendix A** for the checklist to facilitate implementation of such systems.

5.2 Attributes of an Acceptable Electronic Document

| Attributes | Description | Functionality / Remarks |
|---|---|---|
| Integrity | Data are archived and any updates on the technical data are reflected in the document | 1. Computer hardware and software system should store and retrieve the technical data under conditions of normal operation and use.<br>2. The system should not permit unauthorised modification of the data it contains.<br>3. Revisions to the technical data contained in the manual should be current and complete. In addition, revisions should be approved by the appropriate authority before distribution. |
| System Support | Maintenance and support of the Electronic Document | 1. It should include provisions for outages and necessary alternative retrieval services.<br>2. The approval holder or operator is responsible for compliance with all regulatory requirements and cannot be delegated. |
| Accessibility | Distribution of the Electronic Document | 1. Distribution of electronic manual may be similar to distribution of information contained in hardcopies. Approval holders or operators may use their current manual distribution system to distribute electronic documents. |
| Archiving | The electronic recording system are backed up routinely. | 1. The backup system should be robust and reliable.<br>2. There should be a periodic backup schedule that backups the records at pre-determined frequencies to ensure minimum data-loss.<br>3. The recovery of data from the backup should also be demonstrated. |

## 6. PROCEDURES:

6.1 Procedures should be established allowing the organization to correct records/ documents that were electronically signed in error. The original entry should be superseded anytime a correction related to that entry is made. (The original entry should be voided but remain in place. Reference to a new entry should be made and electronically signed and dated). It should be clearly identified that the original entry has been superseded by another entry.

6.2 The system should contain restrictions and procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment which should be properly logged. This should be done immediately upon notification of the change in employment status.

6.3 Procedures should be established to describe how the operator will ensure that the computerized records are transmitted in accordance with the appropriate regulatory requirements to customers or to another operator or to the DGCA or other National Aviation Authority.

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

6.5 Procedures should be established for reviewing the computerized personal identification codes system to ensure that the system remains secure.

6.6 Procedures should be established for auditing the computer system periodically 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 supported by system automatic self- testing.

6.7 Procedures should be established for non-recurring audits of the computer system if the integrity of the system is suspect.

6.8 Audit procedures should be established to ensure the integrity of each computerize 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. The procedures should be applicable to both fixed (e.g. desktop computers) and mobile equipment (e.g. laptops, tablets, PMATs etc.).

6.9 Guidelines should be established for authorised representatives of the owner/operator to use electronic signatures and to have access to the appropriate records.

6.10 Revision Control Procedures

(a) To audit the revision process to ensure contents of the electronic system are current and complete.

(b) To allow approval holders or operators to 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) To ensure that all electronic storage media contain the current revision and associated revision dates.

(d) To ensure users of information or printed data from electronic manual systems obtain the information or printed data from the most current manual.

## 7. TRAINING PROCEDURES:

(a) Training procedures and requirements to authorise access to the computer hardware and software system. Users of the system should also be trained on its proper usage and regularly briefed on security.
(b) 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.

## 8. ARCHIVING PROCEDURES:

(a) To ensure no unauthorised changes can be made to the materials.
(b) To ensure that storage mediums that minimise regeneration of errors or deterioration are selected.
(c) To ensure duplicate technical data are archived at a frequency compatible with the storage life of the medium.
(d) To ensure duplicate copies are stored in physically separate archives to minimise the risk of data loss in the event of a fire or natural disaster.
(e) To ensure future systems are able to retrieve archived technical data. Otherwise, the old system shall be maintained to ensure data availability.

## 9. ORGANISATIONAL REQUIREMENTS:

An Organization intending to implement electronic system(s) for electronic signatures, records or documents should establish a program capable of implementing & maintaining such technologies. To determine how effectively each entity is being assessed (e.g., host, network, procedure, person) and meets the minimum requirement, the Organization should ensure the electronic system should broadly contain the following key elements:

(i) Identification of key personnel in the Organization with authority and overall responsibility for implementing, modifying, revising, and monitoring the electronic system.
(ii) There should be a system defined to ensure compliance and personnel responsible for ensuring the integrity and security of the electronic system and that the process is followed. In addition, there should be a system to allow identification on who is authorized to use the electronic system and for what purposes.
(iii) To provide quality assurance, there should be an auditing process and plan to ensure the requirements for an electronic system continue to be met. The audit procedures should also contain how and when to submit any changes to the processes to DGCA for acceptance prior to implementation.
(iv) Details relating to the training requirements should be defined. The program should define procedures for on-going training of personnel. DGCA may participate in training programs, as required. If the technologies used are novel or first-of-its-kind, training should also be provided for DGCA personnel.
(v) The Organization should define in the relevant exposition manual (and any referenced manuals) how the electronic system(s) would be used or applied throughout their operation in the Organization. There should be description of the hardware and software capabilities for applications of the electronic system(s). The description should also include system support of any computer hardware or software that is part of the electronic system(s).
(vi) Organizations intending to implement an Electronic System for signature, records & documents should initiate a Management of Change (MoC) with regard to identifying/assessing the impact, mitigate and necessary action plans when introducing Electronic Records System in their respective Organizations.
(vii) Organizations intending to implement Electronic Signature, Records/ Documents should establish and retain records, referring to Appendix A to this

AC as guidance:

(a) Records showing compliance to regulations and conformity to this AC. The records must be retained as an evidence.

(b) Statement issued by the Subject Matter Expert (SME) or external organization supplying the IT System to the Organization, declaring that the IT System meets the applicable Standards & Technical Specifications specified in this AC.

## 10. STANDARDS & TECHNICAL SPECIFICATIONS:

The IT system used to generate and/or process an electronic record/ document as well as any associated electronic signature should be developed by considering the applicable provisions of the following Standards & Technical Specifications:

(i) Air Transport Association (ATA) Spec 2000 e-business Specification.
(ii) ATA iSpec 2200 Information Standards for Aviation Maintenance.
(i) ATA Spec 2300 Data Exchange Standard for Flight Operations.
(ii) ATA Spec 2500 Aircraft Transfer Records.
(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.

## 11. OTHER FORMS OF RECORD KEEPING:

Other forms of record keeping acceptable to the DGCA normally means in one of the following formats:

(i) As the original paper form.
(ii) As an electronically digitized copy of the original paper form, or
(iii) As a microfilm or scanned copy of the original form, or
(iv) As a paper form where the paper record is a printed reproduction of an original form from either (i), (ii) or (iii) above.

## 12. SECURITY AUDIT:

For compliance with the provisions of the Information Technology Act, 2000, the security procedure and practices prescribed by the Government for the maintenance, security , storage etc. of electronic data, security audit of the organization electronic record system shall be carried out annually by a third party organization. (Third Party Organisation should be duly affiliated /recognized the CERT-IN/ Government)

Note: *While scanning paper records for the scope of digitization could be encouraged as a bridging solution in the transition from paper based to paperless,*

*there are many limitations compared to "pure digital/electronic" sources. However, based on the merits of the individual case, there are *OCR software products which may provide an interim solution to consider. The OCR of the paper based documents could result in significant document/record electronic capabilities (e.g. key word searching, data mining etc) but just the image of a hand written signature does not necessarily meet in itself the electronic signature requirements.*

**Optical character recognition (OCR) – Software that convert pictures to text. OCR software analyze a document and compare it with fonts stored in their database and/or by noting features typical to characters. OCR creates searchable, editable text from printed documents and also from photos of printed documents, or PDFs made from scanning old documents and papers.*

## 13. REFERENCE PUBLICATIONS:

- CAR 21, CAR M, CAR 145
- The Information Technology Act , 2000
- ICAO DOC 9760 - Amendment (Final Draft)
- EASA NPA 2014-04
- CAAS AC 1-2(1)
- FAA AC 120-78A

**Sd/-**
**(D. C. Sharma)**
**Joint Director General of Civil Aviation**

**Appendix – A**

**ELECTRONIC SIGNATURES / RECORDS / DOCUMENTS – COMPLIANCE / CONFORMITY CHECKLIST:**

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| **(A) SECURE ELECTRONIC SIGNATURES** | | | | |
| 1. | Determine whether the security procedure is reasonable based on:<br>(a) nature of the transaction;<br>(b) sophistication of the parties;<br>(c) volume of similar transactions engaged in by either or all parties;<br>(d) availability of alternatives<br>(e) cost of alternative procedures; and<br>(f) Procedures in general use for similar types of transactions. | Assess whether the means of identification and authentication (e.g. User-ID and password, one-time 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.<br><br>Through control and archives, the system should be capable of determining if the signature is genuine and if the individual is authorised 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. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 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 non-repudiation 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 unauthorised 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. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 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. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 10. | Verify whether specified security procedure or a commercial reasonable security procedure is established to allow the organisation 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 | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| | | use of borders or flashing characters. The system should also notify the signatory that the signature has been affixed. | | |
| 12 | Electronic signature or electronic authentication technique is as specified in the Second Schedule of the Information Technology Act, 2000. | Verify the authentication technique used by the operator vis-à-vis Second Schedule of the Information Technology Act, 2000 | | |
| **(B) SECURE ELECTRONIC RECORDS** | | | | |
| 13. | 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.<br>An electronic record may be a record generated electronically by an electronic transaction, or an electronic image of a paper record. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 14. | 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 unauthorised way. | Check and verify that the system has reasonable security measures to ensure the integrity of the electronic records.<br>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.<br>Corrected errors or alterations to the records need to be identified and the reason for the correction included and reviewed. | | |
| 15. | 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. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 16. | 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. | | |
| 17. | Verify whether there are procedures for making the required records are available. | This procedure and computer system should be capable of making paper and soft copies of the viewed information at the request of DGCA. | | |
| 18. | 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 organization shall retain credentials & ensure competency of the auditor performing audit of the electronic system. | | |
| 19. | Verify whether the application of a specified security procedure or a commercial reasonable security procedure describes how the operator will ensure that the computerised records are | Check whether records comply with DGCA CAR OPS, CAR M, CAR 145, CAR 21 and Licensing Regulation requirements. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| | transmitted in accordance with the appropriate regulatory | (relevant Rules and CARs) | | |
| 20. | 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. | | | |
| 21. | Verify whether there are guidelines for authorised representatives of the owner/operator to use electronic signatures and to have access to the appropriate records. | | | |
| 22. | 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 DOCUMENTS** | | | | |
| 23 | An electronic document shall address the following operational and maintenance requirements:<br>(i) Storage and Retrieval Computer hardware and software system should store and retrieve the technical data under conditions of normal operation and use. The system should not permit unauthorised modification of the data it | | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| | contains.<br>(ii) Maintenance and Support:<br>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.<br>However, the approval holder or operator is still responsible for compliance with all regulatory requirements and cannot be delegated.<br><br>(iii) Access to Document:<br><br>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.<br><br>(iv) 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.<br><br>(v) Revisions to Document | | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 24 | Revision Control Procedures<br><br>(i) Procedures should be established to audit the revision process to ensure contents of the electronic system are current and complete.<br><br>(ii) 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.<br><br>(iii) 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.<br><br>(iv) Users of information or printed data from electronic document systems should ensure the information of printed data is from the most current document. | | | |
| 25 | 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 | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| | | guides and simulated problem-solving exercises. | | |
| 26 | Data Content and Forms of Display<br><br>Computer-displayed information shall contain the following:<br><br>(i) The document title<br>(ii) Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model<br>(iii) Effective date of the data<br>(iv) Revision simultaneously displayed with the technical data<br><br>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.<br>Means of referencing the section or page of the document from which data was obtained should be provided.<br><br>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). | | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 27 | Verify procedures to archive earlier versions of documents to provide for future needs to duplicate, regenerate, or reconstruct maintenance instructions.<br>The archived materials should be obtained from the original source of the data. The procedures should include the following:<br>(i) Ensuring no unauthorised changes can be made.<br>(ii) Selecting storage mediums that minimise regeneration of errors or deterioration.<br>(iii) Duplicate archived technical data at a frequency compatible with the storage life of the medium (before the storage medium deterioration).<br>(iv) Storing duplicate copies in physically separate archives to minimize the risk of data loss in the event of a fire or natural disaster.<br>(v) Future systems should be able to retrieve archived technical data. Otherwise, the old system shall be maintained to ensure data availability. | | | |
| 28 | Verify whether there are procedures to ensure capability of making paper copies of the viewed information at the request of DGCA. | This procedure and computer system should be capable of making paper and soft copies of the viewed information at the request of DGCA. | | |

| S/N | CONTROL STEPS | CHECKS | ORGANIZATION DOCUMENT REFERENCE | Remarks Sat/ Unsat |
|---|---|---|---|---|
| 29. | Parawise compliance of this AC | | | |
| **(D) STATEMENT OF CONFORMITY** | | | | |
| 30. | Statement issued by the Subject Matter Expert or external organization supplying the IT System to the Organization | Declaration that the IT System meets the applicable Standards & Technical Specifications highlighted in this circular. | | |

**-END-**