Civil Aviation Authority of Singapore

Advisory Circular

ELECTRONIC SIGNATURES, RECORDKEEPING AND DOCUMENTS

1. GENERAL. Pursuant to paragraph 88B of the Air Navigation Order, the Director-General of Civil Aviation (DGCA) may, from time to time, issue advisory circulars (ACs) on any aspect of safety in civil aviation. This AC contains information about standards, practices and procedures acceptable to CAAS. The revision number of the AC is indicated in parenthesis in the suffix of the AC number.

2. PURPOSE. This AC is issued to provide guidance and information on the use of electronic signatures, electronic recordkeeping, electronic documents such as manuals, as an alternative to paper-based systems. The holder of CAAS aviation safety instrument (ASI)[1] is guided by this AC for implementation of such electronic systems.

3. APPLICABILITY. This AC applies to holders of a CAAS ASI.

4. CANCELLATION. This AC supersedes AC 1-2(1) dated 9 September 2016.

5. EFFECTIVE DATE. This AC is effective from 03 June 2019.

6. REFERENCES.

- Electronic Transactions Act (Revised Edition 2011);
- Air Navigation Order (ANO);
- Singapore Airworthiness Requirements (SAR);
- Singapore Airworthiness Requirements (SAR) Part-145; and
- Singapore Airworthiness Requirements (SAR) Part-21.

7. BACKGROUND.

7.1 Electronic Transaction Act (ETA) was re-enacted in 2011 to provide for the continuing security and use of electronic transactions in Singapore. One of the key changes was the provisions of technology-specific security procedures such as Public Key Infrastructure (PKI) in the Third Schedule. This AC highlights the new requirements arising from the re-enacted ETA and provides additional guidance on the acceptability of electronic documents.

7.2 CAAS supports the use of electronic systems such as electronic signatures, electronic recordkeeping and electronic documents such as manuals. Such systems may now be used to generate and sign off aircraft records, such as maintenance and manufacturing task cards,

[1] CAAS aviation safety instrument (ASI) means any licence, permit, certificate, authorisation, approval or other document issued by CAAS.

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.

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), Delayed Discrepancies List (DDL), loading or manifest, dispatch release, flight test reports, pilot training records, etc.

7.4 A holder of CAAS ASI ("ASI holder") intending to use electronic system(s) in lieu of paper system(s) should ensure that he has established system level capability at the organisational level reflected in paragraph 8.

8. ORGANISATIONAL LEVEL CAPABILITIES.

8.1 An ASI holder intending to implement electronic system(s) for signatures, recordkeeping or documents should establish a program capable of implementing such technologies. As a minimum, the program should broadly contain the following key safeguards:

(a) Identification of key personnel in the organisation with authority and overall responsibility for implementing, modifying, revising, and monitoring the electronic system. There should 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 should be a system to allow identification on who is authorised to use the electronic system and for what purposes.

(b) 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 process to CAAS for acceptance prior to implementation.

(c) Details relating to the training requirements should be defined. The program should include procedures for on-going training of personnel. If the technologies used are novel or first-of-its-kind, training should also be provided for CAAS officers.

(d) The electronic system should 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

8.2 The ASI holder should explain in his exposition manual (or equivalent) how electronic system(s) would be used or applied throughout their operation. 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).

8.3 Paragraphs 9, 10 and 11 provide more details about security elements for an electronic signature, recordkeeping or document system.

9. ELECTRONIC SIGNATURES.

This paragraph highlights the security requirements for electronic signatures contained in the Electronic Transactions Act (Revised Edition 2011).

9.1 General

An electronic signature's purpose is identical to that of a handwritten signature, and therefore must at a minimum possess those qualities and attributes intrinsic to that of a handwritten signature that guarantee its authenticity. Refer to **Appendix A** for the checklist to facilitate implementation of such system(s).

9.2 Functions and Characteristics of a Signature

A signature is capable of performing a number of functions, namely it can:

(a) Identify the signatory;
(b) Provide certainty as to the personal involvement of a particular person in the act of signing;
(c) Associate a particular person with the contents of the document;
(d) Attest to the intention of a person to be bound by the contents of the document;
(e) Attest to authorship of the document by the signatory; and
(f) Attest to some written agreement which may have been written by some third party who is not a party to the binding agreement.

9.3 Forms of Electronic Signatures

9.3.1 An electronic signature may be broadly identified in the expert field of digital security in accordance with its technological features and capabilities. It can be used as a means of authenticating a record, record entry, or document, and may be in the form of:

(a) Digital signature;
(b) Digitised image of a paper signature; or
(c) Other unique form of individual identification system such as advanced electronic signature, secure electronic signature or digital electronic signature.

9.3.2 A user of electronic signatures should be aware that not all identifying information may constitute an electronic signature. Other guarantees equal to those of a handwritten signature should be provided. Although a signature may take many forms, not all electronic entries may satisfy the criteria to qualify the entry as an acceptable signature. See paragraph 9.5 for the attributes of an acceptable electronic signature.

NOTE: In 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 system application. The onus is on the ASI 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.

9.4 Digital Signatures, Certificates, Public Key Infrastructure (PKI), and Certification Authorities

9.4.1 Digital signature technology is the foundation of a variety of security and electronic transactions. Based on public/private key cryptography, digital signature technology is used in secure messaging, PKI, virtual private networks (VPN), web standards for secure transactions, and electronic standards. Under the Third Schedule of the ETA, the general features of a reliable digital signature, duties of Certification Authority and duties of subscribers are defined accordingly.

9.4.2 Public/private key cryptography encrypts and decrypts data through the unique pairing of public and private keys. Private keys are kept secret and stored in a protected environment, whereas public keys are housed in publicly accessible directories for use in decrypting messages. Digital signatures verify the origin of digitally signed data using a public key to confirm that the data was encrypted with a private key. When combined with a hashing algorithm, digital signatures can also verify the integrity of data.

9.4.3 Digital signature technology may not enable individuals to sign electronic data with the same effect as a handwritten signature. For this to occur, digital signature technology must be incorporated into a process that reproduces the basic elements of a handwritten signature. .

9.4.4 While the public and private key pairs used in a digital signature are unique and can authenticate data for a very simple process, signing applications are not simple processes. Without a process or an application, a digital signature on its own cannot electronically reproduce the key elements required of a binding handwritten signature.

9.4.5 When digital signature technology is used to authenticate a particular individual, that individual's public key is digitally signed with another private key to secure his/her identity. This process produces what is known as a digital certificate, which can be issued and managed in one of two ways: It can be self-issued or issued through a Public Key Infrastructure (PKI).

9.4.6 A self-issued certificate (not acceptable to CAAS), also known as self-signed certificate, is produced when an individual signs his/her own certificate. The equivalent of a handwritten signature on paper, a self-signed certificate means the bearer alone can vouch for the authenticity of his/her identity. In these cases, verification of that identity occurs directly between the individual in question and the other parties involved in the transaction. Once approved, subsequent use of the individual's digital certificate can be trusted.

9.4.7 While self-issued certificates are the easiest to implement and manage, digital certificates using PKI (acceptable to CAAS) 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 organisation, 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 person or department within an organisation, or by a trusted third party acceptable to CAAS, preferably an accredited Certification Authority as defined in the Third Schedule of ETA. The Certification Authority shall assume the liability of vouching for an individual's identity.

9.5 Attributes of an acceptable electronic signature

Attributes	Description	Functionality / Remarks
Signature Security and Uniqueness	An electronic signature is unique by retaining qualities of a handwritten signature that is difficult to duplicate or alter. It should be able to identify a specific individual with reasonable certainty	1. It provides evidence that an individual agrees with a statement. 2. There shall be an identification and authentication procedure that validates the identity of the signatory based on uniqueness of the signature. 3. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. 4. An individual using an electronic signature shall be required to identify himself or herself, and the system that produces the electronic signature should then authenticate that identification. 5. The system shall be able to prevent an unauthorised individual from certifying required documents, such as certificate of release to service.
Traceability	An electronic signature provides positive traceability to the individual who signed a record, record entry, or any other document for accountability purposes.	1. There shall be procedures to positively identify a person who sign a record, or any other document for accountability purposes. 2. There shall be means to track all changes made to the electronic records and ensure that these changes are periodically reviewed.

Significance	An individual using an electronic signature takes deliberate and recognisable action to affix his or her signature.	1. Acceptable, deliberate actions for creating a digital electronic signature include, but are not limited to, badge swipes, signing an electronic document with a stylus, typing specific keystrokes, or using a digital signature.
Scope	The scope of information being affirmed with an electronic signature is clear to the signatory and to subsequent readers of the record, record entry, or document. CAAS is not concerned with the computer technology used to accomplish the tasks. Instead, CAAS' concern is with the accuracy of the record and that the signatory is fully aware of what he or she is signing.	1. The user should be asked to ensure that the identified material is, in fact, what is being signed. 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. 2. 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.
Non-repudiation	An electronic signature prevents a signatory from denying that he or she has affixed a signature to a specific record, record entry, or document	1. The more difficult it is to duplicate a signature, the likelier the signature was created by the signatory.

9.6 System requirement for electronic signature system

A system implementing electronic signatures must have the following features:

(a) Signature authenticity/verification: Through control and archives, the system must 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.

(b) Archiving electronically signed documents: A means of safely archiving electronically signed documents must be part of any electronic signature computer software.

(c) 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.

(d) Procedures must be established allowing 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. (The entry should be voided but remain in place. Reference to a new entry should be made and electronically signed and dated).

(e) In general, the Electronic Transaction Act does not limit organisations to only use secure electronic signatures. However, when secure electronic signatures based on Public Key Infrastructure technology is not used, additional security procedures such as use of fingerprint, PINs or any equivalent alternatives with the electronic signature are recommended. Security of such electronic signatures, in this case, will be comparable to secure electronic signatures.

10. ELECTRONIC RECORDKEEPING.

10.1 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 implementation of such systems.

10.2 Attributes of an Acceptable Electronic Recordkeeping 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. 2. Identification and authentication procedures can be implemented to enhance security. 3. The system is capable of ensuring that the information is not altered in an authorised 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. 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. 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. 2. There should be a periodic backup schedule that backups the records at pre-determined frequencies to ensure minimum data-loss. 3. The recovery of data from the backup should also be demonstrated.

10.3 Procedures

Before introducing an electronic recordkeeping system, the following procedures should be established:

(a) Record Transmission Procedures

(i) Procedures to ensure that the computerised records are transmitted in accordance with the appropriate regulatory requirements to customers or to another operator in a format acceptable to them.

(ii) 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.

(b) Audit Procedures

Procedures to audit the computer system annually to ensure 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 for one of each type. The remediation for the sampled component should then be propagated to the rest of the non-sampled ones.

(c) Availability of Records to Relevant Authorities

Procedures to ensure the capability of making paper copies of the viewed information is available at the request of CAAS and Transport Safety Investigation Bureau (TSIB) of Ministry of Transport (MOT).

(d) Security Procedures

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

(e) Archiving Procedures

(i) To ensure no unauthorised changes can be made to the materials.

(ii) To ensure storage mediums that minimise regeneration of errors or deterioration are selected.

(iii) To ensure duplicate technical data are archived at a frequency compatible with the storage life of the medium.

(iv) 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.

(v) To ensure future systems are able to retrieve archived technical data. Otherwise, the old system shall be maintained to ensure data availability.

(f) Training Procedures

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 ICT (Infocomm Communication & Technology) security.

11. ELECTRONIC DOCUMENTS.

11.1 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.

11.2 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. 2. The system should not permit unauthorised modification of the data it contains. 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. 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. 2. There should be a periodic backup schedule that backups the records at pre-determined frequencies to ensure minimum data-loss. 3. The recovery of data from the backup should also be demonstrated.

11.3 Procedures

Before introducing an electronic document system, procedures should be established, including:

(a) Revision Control Procedures

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

(ii) 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.

(iii) To ensure that all electronic storage media contain the current revision and associated revision dates.

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

(b) Archiving Procedures

(i) To ensure no unauthorised changes can be made to the materials.

(ii) To ensure that storage mediums that minimise regeneration of errors or deterioration are selected.

(iii) To ensure duplicate technical data are archived at a frequency compatible with the storage life of the medium.

(iv) 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.

(v) To ensure future systems are able to retrieve archived technical data. Otherwise, the old system shall be maintained to ensure data availability.

(c) Availability of Records to Relevant Authorities

Procedures to ensure the capability of making paper copies of the viewed information is available at the request of CAAS and the Transport Safety Investigation Bureau (TSIB) of Ministry of Transport (MOT).

(d) Training Procedures

(i) Training Programs should be provided to employees who use the Electronic Manual.

(ii) 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.

11.4 Consideration in Displaying Information

Information retrieved from an electronic manual might be displayed in a different format than it appears on hardcopies. However, the information should be identical in content regardless of its format. Any computer-displayed information should be readily accessible to the user and should be able to obtain the following:

(a) The manual title
(b) Relevant aircraft component model
(c) Effective date of the data
(d) Revision simultaneously displayed with technical data
(e) Table of revision

APPENDIX A

ELECTRONIC SIGNATURES/RECORDS/DOCUMENTS COMPLIANCE CHECKLIST

S/N	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, 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. 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.
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.
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 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 use of borders or flashing characters. The system should also notify the signatory that the signature has been affixed.
(B)	**<u>SECURE ELECTRONIC RECORDS</u>**	
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 unauthorised 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 required records available to CAAS officers and the Transport Safety Investigation Bureau (TSIB) of Ministry of Transport (MOT).	This procedure and computer system should be capable of making paper and soft copies of the viewed information at the request of CAAS and the TSIB 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 CAAS' 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 computerised 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 AOC, SAR145 and SAR21 requirements.
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 authorised 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 DOCUMENTS		
22	An electronic document shall address the following operational and maintenance requirements: 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 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.	
23	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.	
24	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.

25	<u>Data Content and Forms of Display</u> 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 <u>Page Numbers and Revision Data</u> 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).	
26	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 unauthorised changes can be made (b) Selecting storage mediums that minimise 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.	
27	Verify whether there are procedures to ensure capability of making paper copies of the viewed information at the request of CAAS and the TSIB of MOT.	This procedure and computer system should be capable of making paper and soft copies of the viewed information at the request of CAAS and the TSIB of MOT.