CIVIL AVIATION AUTHORITY OF NEW ZEALAND
Te Mana Rererangi Tūmatanui o Aotearoa

Advisory Circular AC00-6

Revision 1

10 August 2022

Electronic Signatures, Electronic Record-keeping and Electronic Manuals

General

Civil Aviation Authority (CAA) advisory circulars (ACs) contain guidance and information about standards, practices, and procedures that the Director has found to be an acceptable means of compliance with the associated rules and legislation.

Consideration will be given to other methods of compliance that may be presented to the Director. When new standards, practices, or procedures are found to be acceptable they will be added to the appropriate AC.

Purpose

This AC describes an acceptable means of compliance with requirements for electronic signature, electronic record keeping, and electronic manual systems/programs. While all three have been addressed in the one AC, there is no requirement for a participant to include all three in their organisation, as any combination is acceptable.

It is the participant's responsibility to address all the requirements of the Civil Aviation Rules as well as the requirements of the Contract and Commercial Transactions Act. This AC applies to aviation document holders who seek to incorporate electronic signature, record keeping or manual systems and programs into their operations.

Related Rules

This AC relates specifically to various Civil Aviation Rules identified in Appendix A.

Change Notice

This AC cancels revision 0.1 of AC00-6, dated 7 April 2021. Revision 1 corrects an inaccurate reference to AC43-1, in Appendix A, p 17.

Version History

History Log.

Revision No.	Effective Date	Summary of Changes
0	20 July 2020	The initial issue of this AC.
0.1	7 April 2021	Removed a duplicate entry in the Definitions section
1	10 August 2022	Corrects an inaccurate reference to AC43-1, in Appendix A, p 17.

Table of Contents

1) Definition

1.1 The following terms are used in this AC.

Authentication means by which a system validates the identity of an authorised user. These may include a password, a personal identification number (PIN), a cryptographic key, smart card and so on. These means may be combined (for example a cryptographic card and a PIN) for increased confidence in the identity of the system user.

Computer-based record keeping system means a system of record processing in which records are entered, maintained, archived, and retrieved electronically. The term “computer-based record keeping system” is synonymous with “electronic record keeping system.”

Data backup means use of one of several recognised 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, failure, or damage to the primary record keeping system.

Data storage device means any article or device (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device.

Data verification means a process of ensuring accuracy of data records by systematically or randomly comparing electronic records with manual data entry documents.

Digital Signature means cryptographically generated data that identifies a document’s signatory, with date and time. The result of which, when properly implemented, provides the services of original authentication, data integrity, and signer non-repudiation.

Electrical system consists of an electrical power source, its power distribution system and the electrical load connected to that system**.**

Electronic includes electrical, digital, magnetic, optical, electromagnetic, biometric, and photonic.

Electronic communication means a communication by electronic means.

Electronic manuals means aviation document holder manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, internet/intranet-based, or various other forms of electronic media, to include commercial off-the-shelf portable electronic device (PED) hardware (for example laptop, tablet, phone, and so on).

Electronic record means contract or other record created, generated, sent, communicated, received, or stored by electronic means.

Electronic record keeping system means a system of record processing in which records are entered, signed, stored, and retrieved electronically. The term “electronic record keeping system” is synonymous with “computer-based record keeping system.”

Electronic signature means functionally equivalent to a handwritten signature. It is an electronic 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.

Information includes information (whether in its original form or otherwise) that is in the form of a document, a signature, a seal, data, text, images, sound, or speech.

Information system means a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications.

Password means an identification code or device required to access stored material, intended to prevent information from being viewed, edited, or printed by unauthorised persons.

Return to service: abbreviated as RTS.

Signature means a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation, and to authenticate a record entry. A signature should be traceable to the individual making the entry, and it should be handwritten or part of an electronic signature system.

2) Approval, acceptance, and authorisation

2.1 There are many Civil Aviation Rules that address signatures, records/record keeping, and manuals. Appendix A lists those Civil Aviation Rule parts that are impacted by electronic signatures and data storage systems. As there are varying requirements for the approval, acceptance, and authorisation of electronic record keeping and electronic manual systems, CAA will use the exposition approval method to indicate that approval or acceptance.

2.3 The information in this AC relates only to CAA's acceptance guidelines for electronic signature, electronic record keeping, and electronic manual systems/programs. It is not considered an approval or authority for participants to use any particular software, only that CAA has no objections as long as the process meets certain requirements. Each aviation business has its own unique framework of legislative responsibility and, additionally, certain manufacturers prohibit the maintenance records for their products being delivered in digital form. With this in mind, it is the participant's responsibility to determine their obligations to all business stakeholders, prior to considering the use of such products. Furthermore, if a participant is considering outsourcing the provision and management of an electronic record keeping or electronic manual systems to a third party then a written declaration should be sought from that provider confirming the applicable requirements called out in this AC are met.

2.4 In the absence of its own regulations, CAA relies heavily on Part 4 of the New Zealand Contract and Commercial Law Act 2017 (CCLA). This is because any policy regarding electronic signatures and data storage systems must comply with this legislation regardless of the context in which it is used. Appendix B lists those provisions of the CCLA that are relevant to the types of products being proposed to support electronic signatures and alternatives to paper based systems, as well as some examples of what should be considered. Participants are encouraged to read and review them to ensure any proposed systems meet all the relevant requirements.

3) Electronic signatures

3.1 **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 CAA; therefore, electronic signatures must possess those qualities and attributes that guarantee a handwritten signature's authenticity.

(a) Types of Electronic Signatures. Electronic signatures may appear in various formats and must meet the requirements in 3.1(c). Examples of electronic signature formats include, but are not limited to:

(i) A digitised image of a handwritten signature that is attached to an electronic record;

(ii) An electronic code (e.g., a secret code, password, or personal identification number (PIN)) used by a person to sign the electronic record;

(iii) A unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan; or

(iv) A digital signature.

(b) Electronic Signature Standards. Electronic signatures should meet the following criteria to be considered legally binding.

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

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

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

(iv) 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.

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

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

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

(viii) 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).

(c) Digital Electronic Signatures. Digital signatures are electronic signatures that incorporate encryption and decryption technology. They are typically the most secure and are based on Public and Private Key Infrastructure (PKI) and utilise digital certificate authentication. This technology 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.

3.2 **Electronic Signature Process.** A participant'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 username 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:

(i) "Signed by,"

(ii) "Certified by,"

(iii) "Instructor's signature/certification,"

(iv) "Signature,"

(v) "Authorised by,"

(vi) "Signatory,"

(vii) "Authentication,"

(viii) "Acknowledged by,"

(ix) "Acknowledgement," and/or

(x) "Affirmed by."

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

(i) Using a digital signature;

(ii) Entering a username and password;

(iii) Swiping a badge; and/or

(iv) 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:

(i) 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.

(ii) 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 Unauthorised Access and Modification. An electronic signature process must be secure and must prevent unauthorised 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 unauthorised individuals from certifying required documents. 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 always under the sole custody of the signatory.

3.3 **Policies and Procedures.** When constructing an electronic signature process, the exposition should include the following elements:

(a) Description of Electronic Signature Process. The description should explain how electronic signatures will be used and how electronic signatures are applied throughout the organisation.

(b) Policies and procedures identifying who has 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.

(c) Identification of Persons Authorised to Use Electronic Signatures. Participants must have a system for identifying who is authorised to use the electronic signature process, for what purposes, and which records.

(d) 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. This includes controlling revision state/version history of the software or application, and ensuring statutory responsibilities continue to be met for any system changes.

(e) 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 unauthorised event recognition, which includes actions to be taken by the participant upon discovery of an attempt by an unauthorised individual to use an electronic signature.

(f) Data Backup and Retention. Policy and procedures should address how data backup and retention of data will be accomplished. Refer Section 6 below for additional considerations.

(g) 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.

(h) Training and User Instructions. A participant’s policies and procedures should include any training and instructions necessary to ensure authorised 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.

4) Electronic record keeping

4.1 **General**. 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. Examples of electronic records include, but are not limited to:

(a) Maintenance activities

(b) Pilot maintenance

(c) Daily flight records, including weight and balance, and flight and duty

(d) Training records

(e) Drawings

4.2 **CAA Standards for Electronic Records**. To be considered complete and valid, an electronic record should contain at least the following information:

(a) The type of event that took place (e.g., training, maintenance performed, signing of a release, conduct of a flight, etc.);

(b) Where required information that shows compliance with regulatory requirements (e.g., for a training activity the name of the course module or subject, the number of hours of instruction, whether the student passed or failed, etc);

(c) When the event took place (e.g., the date and time (where appropriate));

(d) Where the event took place (e.g., the station, training facility, maintenance facility, etc.);

(e) Who was involved in the event (e.g., crewmember, dispatcher, instructor, mechanic, etc.);

(f) Aircraft type and registration number for pilot logbook records (when required by rules);

(g) Certification, verification, or authentication, such as a signature (when required by rules); and

(h) Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model for maintenance records, such as life-limited parts and time-in-service records.

4.3 **Security**. The electronic record keeping system should:

(i) Protect confidential information.

(ii) Ensure that the information in an electronic record is not altered in an unauthorised way.

(iii) Provide for secure access and contain safeguards against unauthorised access.

4.4 **Policies and Procedures.** When constructing an electronic record keeping system, the exposition should include the following elements:

(a) Description of Electronic Record keeping System(s). The description should explain how the electronic record keeping system(s) will be used throughout the organisation. This includes identifying those records that will be maintained in the electronic system(s).

(b) Policies and procedures identifying who has the authority and overall responsibility for the integrity and security of the electronic record keeping 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, revising, and monitoring the electronic record keeping system, as well as those who are responsible for entering data into the system.

(c) Persons with Authorised Access. Participants must have a system for identifying who is authorised to use the electronic record keeping system, for what purposes, and which records.

(d) Description of System Support. Policies and procedures should address system support of any computer hardware or software that is part of the electronic record keeping system. This includes controlling revision state/version history of the software or application, and ensuring statutory responsibilities continue to be met for any system changes.

(e) Audit Procedures. The participant 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 record keeping system continue to be met. Procedures should include unauthorised event recognition, which includes actions to be taken by the participant upon discovery of an attempt by an unauthorised individual to access and/or make entries into the electronic record keeping system.

(f) Data Backup and Retention. Policy and procedures should address electronic system 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 CAA. Refer Section 6 below for additional considerations.

(g) Record Transfer. Procedures should ensure that records transferred with an aircraft (either electronic or on paper) meet applicable rule requirements.

(h) Electronic Authentication, Signature, Validation, or Endorsement. Most records 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.

(i) Transferring Data. Technological advances may make it desirable or necessary for a participant to update their electronic record keeping 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 records are moved from one system to another. This could entail running redundant systems for a brief period of time.

(j) 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.

(k) Continuity of Records for Maintenance Providers. Procedures should ensure continuity with maintenance providers. Participant 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 record keeping system.

(l) Procedures for making required records available to CAA in a format and manner that is acceptable to CAA.

(m) Training and User Instructions. Each electronic record keeping 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 authorise access to the electronic record keeping system.

5) Electronic manual systems

5.1 **General**. 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. 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 CAA approval (e.g., signature or stamp) for those manuals or manual sections that require CAA approval
- Chapter numbers
- Chapter headings
- Section numbers
- Topic headings
- Page numbers
- Applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (when applicable for minimum equipment list (MEL) and maintenance purposes), and
- The person with the authority and responsibility for manual content.

5.2 **Electronic Manual System**. An electronic system for delivering manual content must comply with rule requirements for currency, availability, and distribution to the appropriate personnel. An electronic manual system should address:

(a) Currency. A means 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 CAA.

(c) MEL. A means to provide flight crew with MEL through printed or other means approved by CAA. An Electronic Flight Bag (EFB) is an example of other means that may be approved by CAA.

(d) Security Protocols and Prevention of Unauthorised Access and Modification. Manual system computer hardware and software must prevent unauthorised access and/or modification to electronic manual content.

(e) 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 unauthorised modification of the data it contains.

(f) 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.

(g) 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.

(h) Revision Control. A participant’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:

(i) 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.

(ii) 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.

(iii) 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.

(iv) 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.

(v) Distribution and Submission of Electronic Revisions to CAA.

- Revision control procedures should include the participant’s method of distributing electronic revisions to CAA.
- When a particular manual requires CAA approval or acceptance, the participant’s procedures should explain how the electronic manual will be submitted to CAA.

(i) 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 authorised display device. Information displayed on any authorised device on the flight deck must correlate to information displayed at an authorised computer workstation or authorised 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.

(j) Data Archiving. An electronic manual system should have a method of archiving technical and procedural data superseded by revision. A participant should archive earlier versions of manuals to provide for future needs to duplicate, regenerate, or reconstruct instructions.

(i) The Importance of Historical Data. Archived historical data is particularly important for the following reasons:

- To trace aircraft repair information or reconstructing maintenance instructions.
- To evaluate normal and abnormal flight deck (cockpit) checklist procedures.
- For training purposes.
- For investigation purposes in the event of an accident, incident, or occurrence.

(ii) 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 method of ensuring that no unauthorised changes can be made.
- A method or medium that minimises the deterioration of data.
- A method to protect the archived data against hazards and natural disasters.

(k) Electronic master manuals must include at least the following:

(i) 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.

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

(iii) 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.

(iv) 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 kind 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.”

5.3 **Policies and Procedures.** When constructing an electronic manual system, the exposition should include the following elements:

(a) Description of Electronic Manual System. The description should explain how the electronic manual system will be used throughout the organisation. This includes identifying which manual will be maintained within the electronic system.

(b) Policies and procedures identifying who has the authority and overall responsibility for the integrity and security of the electronic manual 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, revising, and monitoring the electronic manual system, as well as those who are responsible for amending electronic manual within system.

(c) Persons with Authorised Access. Participants must have a system for identifying who is authorised to use the electronic manual system, for what purposes, and which manuals.

(d) Description of System Support. Policies and procedures should address system support of any computer hardware or software that is part of the electronic manual system. This includes controlling revision state/version history of the software or application, and ensuring statutory responsibilities continue to be met for any system changes.

(e) Audit Procedures. The participant must have auditing procedures that ensure the quality and integrity of each electronic manual maintained within the system and that all of the requirements of the electronic manual system continue to be met. Procedures should include unauthorised event recognition, which includes actions to be taken by the participant upon discovery of an attempt by an unauthorised individual to access and/or make entries into the electronic manual system.

(f) Data Backup and Retention. Policy and procedures should address 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 authorised system; the use of backup media such as print or CD-ROM; or other method acceptable to CAA. Refer Section 6 below for additional considerations.

(g) Transferring Data to Another System. Technological hardware or software advances may make it desirable and/or necessary for a participant to update their electronic manual system. When transferring manual data from one electronic system or application to another, participants 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.

(h) User Instructions and Training. Each participant 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.

6) Civil Aviation Rules – retention of records

6.1 The Civil Aviation Rules impose certain requirements on operators to retain maintenance and logbook records for a certain period of time. In light of these requirements, participants must demonstrate how they will access records in the following scenarios:

(a) CAA is aware of certain development agreements where the developer continues to own the intellectual property (IP) and leases it to the service provider as a way of keeping programming and development costs down. The participant must confirm who owns the IP that underpins the application and how the product will continue to run with another developer if the original software developer ceases to support the software.

(b) Assuming the product is cloud based or the storage capability is outsourced, would the participant or their service provider still be able to access the files stored within the database servers if the database provider becomes insolvent, or if overseas governments choose to seize database assets? The participant should state whose insolvency or ownership laws apply in that situation, considering their data will likely be held offshore and multiple jurisdictions' laws will apply.

(c) If the service provider becomes insolvent, would the developer and database provider continue to support the product? How would CAA retain access to these records? How would aircraft owners ensure they could forward a complete set of records with the aircraft when sold?

(d) If new owners of an aircraft previously maintained using the service no longer wish to use the service, how will the records of previous work be archived and accessed by auditors and/or investigators in the future?

(e) If the participant itself becomes insolvent or decides to cease trading, how does CAA ensure it retains access to records held in the participant's name with their service/database providers?

APPENDIX A: Affected Civil Aviation Rules

(a) The following parts have been reviewed: 12, 19, 26, 39, 43, 47, 91, 119, 135, 137, 141, 145, 146, 147 and 148.

(b) Not all reviewed rules had provisions that are impacted by electronic signatures, electronic record keeping and electronic manuals. The affected rules are included in the tables below.

(c) As well as rules directly impacted by electronic signatures, electronic record keeping and electronic manuals, rules that outline how CAA maintains oversight through either Directors approval or acceptance have also been included.

A1.1 Part 19 *Transition Rules*

Rule 19.321(b)(5) Supply control procedures	Requires Director's approval of system for certification of release notes. If electronic system is to be used, this is then approved by Director.

A1.2 Part 43 *General Maintenance Rules*

Rule 43.69(a) and (b) Maintenance records	Rule requires use of "appropriate" logbooks. AC43-1 *Aircraft Maintenance* para 2.14 explains the minimum requirements for maintenance records. If electronic records are used in place of CAA Logbooks, the entries into the electronic system must continue to satisfy the requirements of CAR 43.69. The use of electronic records in place of CAA Logbooks, must be approved by the Director.
Rule 43.69(c) Maintenance records	(1) Mentions release-to-service (RTS) of defect rectification in the technical log. This must form part of the exposition submitted for acceptance by the director, if it is to be in electronic form. Ref also 91.619. (2) and (3) refer to the requirements in 43.69(a) and (b).
Rule 43.69(d)(2) Maintenance records	This states that a signature is required to certify RTS, *"except"* where electronic records are used. This does not negate the fact that such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b). To clarify, any exemption from attaching a symbol as an electronic signature, as defined by this AC, only extends to the use of digital signatures.
Rule 43.103(c)(2)(ii) Requirements for certifying release-to-service	This states that a signature is required to certify RTS for an operational check flight in the logbook or worksheet and technical log, *"except"* where electronic records are used. This does not negate the fact that such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b). To clarify, any exemption from attaching a symbol as an electronic signature, as defined by this AC, only extends to the use of digital signatures.

Rule 43.105(a)(2) Certifying release-to-service after maintenance	This states that a signature is required to certify RTS after maintenance in the logbook or worksheet and technical log, *"except"* where electronic records are used. This does not negate the fact that such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b). To clarify, any exemption from attaching a symbol as an electronic signature, as defined by this AC, only extends to the use of digital signatures.
Rule 43.105(b)(1) Certifying release-to-service after maintenance	This states that, for components defined in CAR, Part 43.54 or exported by CAR, Part 145, or Part 148 certificated organisations, a signature is required to certify RTS on a Form 1. If Form 1s are to be in digital form, such a record keeping system needs to be accepted by the Director, as outlined in 145.67(c) and 148.67(b).
Rule 43.105(b)(2) Certifying release-to-service after maintenance	This states that, for components that aren't fitted to aircraft, a signature is required to certify RTS on a Form 2. If Form 2s are to be in digital form, such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b).
Rule 43.109(3)(i) Defects	This states that any defects that remain un-cleared after maintenance checks are entered into the logbooks and/or technical log and that a signature is required to certify that the aircraft is *not* released to service. Ref 43.69(a)(b) and (c).
Rule 43.113(d)(2) Duplicate safety inspection control system	This states that a signature is required to certify duplicate inspections in the logbook or worksheet, *"except"* where electronic records are used. This does not negate the fact that such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b). To clarify, any exemption from attaching a symbol as an electronic signature, as defined by this AC, only extends to the use of digital Signatures.
Rule 43.155(a)(2)(ii) Certifying review	This states that a signature is required to certify RTS for a review of airworthiness in the logbook, *"except"* where electronic records are used. This does not negate the fact that such a record keeping system needs to be accepted by the Director, as outlined in 43.69(a) and (b). To clarify, any exemption from attaching a symbol as an electronic signature, as defined by this AC, only extends to the use of digital signatures.

A1.3 Part 91 *General Operating and Flight Rules*

Rule 91.607(a) Approval of maintenance programmes	References Part 91.605(a)(2) and requires Director's approval of Part 119 maintenance programs.
Rule 91.607(b) Approval of maintenance programmes	Gives requirements for maintenance programs that are to be approved under 91.607(a). Any electronic record keeping process that is outlined in this paragraph is then subject to approval by the Director.

Rule 91.616(1) Maintenance logbooks	Requires “appropriate” logbooks to be provided. Refer 43.69(a) and (b).
Rule 91.617(d) Maintenance records	Says that records may be kept in “encoded” form, but references the information in 91.617(a)(b) and (c), which in turn refer to the record keeping systems in 43.69. Thus, this “encoded” form of record keeping must be accepted by the Director under CAR and AC43.69. Refer 43.69(a) and (b).
Rule 91.619(a) and (c) Technical log	Gives requirements for technical log data and states that the Director’s acceptance must be gained prior to any holder of a 119 certificate using a medium for recording signature bearing technical log data that is different to the normal CAA approved system.
Rule 91.621 Transfer of maintenance records	States all maintenance records in 91.617(a) and (b) must be transferred with aircraft ownership. This then impacts on the requirements of any signature bearing record keeping systems that are accepted by the Director, under 43.69(a) and (b).
Rule 91.623 Retention of records	States all maintenance records must be retained for specified periods. This then impacts on the requirements of any signature bearing record keeping systems that are accepted by the Director, under 43.69(a) and (b).

A1.4 Part 100 *Safety Management*

Rule 100.3(b) System for safety management	The SMS element 2, ERP must integrate any measures to quarantine records held in externally managed databases and include them in any safety investigation carried out IAW element 6. Further, if any other SMS elements utilise external service providers to operate (such as risk management apps), the SMS must reference how this is managed.

A1.5 Part 119 *Air Operator Certification*

Rule 119.15(b)(8) Operations Specifications	The Director may include details of a participant’s management system in the operations specifications.
Rule 119.51(b) Personnel requirements	Airline operator must establish who has responsibility for oversight and maintenance of the system and submit as part of the exposition for acceptability.
Rule 119.81(a) and (b) Airline air operator exposition	Airline operator’s exposition must contain all information required by CAR 119 and be acceptable to the Director, this includes details of all document and record management systems that may be held in electronic form.
Rule 119.101(b) Personnel requirements	General Aviation Air Operator must establish who has responsibility for oversight and maintenance of the system and submit as part of the exposition for acceptability.

Rule 119.125(a) and (b) General aviation air operator exposition	General Aviation Air Operator's exposition must contain all information required by CAR 119 (including maintenance program that shall include a description of the system used to record maintenance activity and retain those records) and that expositions must be acceptable to the Director.
Rule 119.151(b)(ii) Continued compliance	Type and format of stored exposition must be acceptable to Director.

A1.6 Part 135 *Air Operations – Helicopters and Small Aeroplanes*

Rule 135.415(c) Maintenance review	Requires that continuous maintenance review systems that form part of airline maintenance programs are acceptable to the Director.
Rule 135.415(d)(3) Maintenance review	Requires that signature be affixed to maintenance reviews for those carried out under the privileges of a CAR 135 certificate. If these are certified electronically, these systems must form part of an exposition that is acceptable to the Director, under CAR 119.
Rule 135.803(a)(4) Operator responsibilities	CAR 135 Operator's flight and duty schemes must be acceptable to the Director. Any electronic application used to record, track or advise such a scheme must also be acceptable and forms part of the certification requirements in CAR 119.
Rule 135.857(a) and (b) Daily flight record	Defines the information that must be available as part of a daily flight record for each flight. Any electronic application used to record, track or advise such a scheme must also be acceptable to the Director and forms part of the certification requirements in CAR 119.
Rule 135.857(c) Daily flight record	States which daily flight record information is to be made available to the pilot, prior to flight. Any electronic application used to record, track or advise such a scheme must also be acceptable to the Director and forms part of the certification requirements in CAR 119.
Rule 135.859(d) Retention period	Document retention requirements for daily flight records. Any electronic application used to record, track or advise such a scheme must also be acceptable to the Director and forms part of the certification requirements in CAR 119.

A1.7 Part 141 *Aviation Training Organisations Certification*

Rule 141.63(b) Standard aviation training organisation exposition	A certificated Training Organisation's exposition must contain all information required by CAR 141.63(a) and be acceptable to the Director, this includes details of all document and record management systems that may be held in electronic form.

A1.8 Part 145 *Aircraft Maintenance Organisations Certification*

Rule 145.11(a) Privileges of certificate holder	Allows certificated Maintenance Organisations to perform maintenance on and release to service aircraft and components, as outlined in their exposition, and to issue release notes under Part 19. Refer 119.321(b)(5).
Rule 145.55(2) Equipment, tools, and material	A certificated Maintenance Organisation's exposition must contain procedures for control and calibration of specialist tools. If these are calibrated under procedures included in the exposition and certified in electronic form, this system's function must be documented in the exposition. Refer 145.67(c).
Rule 145.59(b)(6) and (7) Maintenance control procedures	This requires an applicant to develop procedures for release-to-service of aircraft or components and to issue authorisations for certification of Form 1's. If these are handled in electronic form, this must be documented in the exposition. Refer 145.67(c) and 43.105(b)(1).
Rule 145.63(a) Records	This requires an applicant to establish procedures for management of records to ensure a product or component is fit for release-to-service. If these are handled in electronic form, this must be documented in the exposition. Refer 145.67(c).
Rule 145.67(a)(8)(vii), (x) and (xv) Maintenance organisation exposition	A certificated Maintenance Organisation's exposition must contain procedures for performance of maintenance activities, release-to-service of aircraft and components, and handling of records. If these are handled in electronic form, this must be documented in the exposition.
Rule 145.67(c) Maintenance organisation exposition	A certificated Maintenance Organisation's exposition must be acceptable to the Director.

A1.9 Part 146 *Aircraft Design Organisations Certification*

Rule 146.55(2) Equipment, tools, and data	A certificated Design Organisation's exposition must contain procedures for control and calibration of specialist tools. If these are calibrated under procedures included in the exposition and certified in electronic form, this system's function must be documented in the exposition. Refer 146.67(b).
Rule 146.59(b)(5) and (6) Design control procedures	This requires an applicant to develop procedures for issuing statements of compliance and design change approvals. If these are handled and certified in electronic form, this must be documented in the exposition. Refer 146.67(b).
Rule 146.63(a) Records	This requires an applicant to establish procedures for management of records to ensure that each design or design change conforms to applicable design data. If these are handled in electronic form, this must be documented in the exposition. Refer 146.67(b).

Rule 146.67(b) **Design organisation exposition**	A certificated Design Organisation's exposition must be acceptable to the Director.

A1.10 Part 148 *Aircraft Manufacturing Organisations Certification*

Rule 148.11 **Privileges of certificate holder**	Allows certificated Manufacturing Organisations to manufacture aircraft and components, as outlined in their exposition, and to issue release notes under part 19. Refer 119.321(b)(5).
Rule 148.55(2) **Equipment, tools, and material**	A certificated Manufacturing Organisation's exposition must contain procedures for control and calibration of specialist tools. If these are calibrated under procedures included in the exposition and certified in electronic form, this system's function must be documented in the exposition. Refer 148.67(b).
Rule 148.59(b)(7) **Production control procedures**	This requires an applicant to develop procedures for issuing Form 1 release certificates. If these are handled and certified in electronic form, this must be documented in the exposition. Refer 148.67(b).
Rule 148.63(a) **Records**	This requires an applicant to establish procedures for management of records to ensure that each design or design change conforms to applicable design data. If these are handled in electronic form, this must be documented in the exposition. Refer 148.67(b).
Rule 148.67(b) **Manufacturing organisation exposition**	A certificated Manufacturing Organisation's exposition must be acceptable to the Director.

APPENDIX B: Contract and Commercial Law Act 2017[1], Part 4, Electronic transactions

B1.1 s213 Time of dispatch

(a) An electronic communication is taken to be dispatched at the time the electronic communication first enters an information system outside the control of the originator.

(b) For the purposes of this section and section 214, information system means a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications.

B1.2 s214 Time of receipt

(a) An electronic communication is taken to be received:

(i) in the case of an addressee who has designated an information system for the purpose of receiving electronic communications, at the time the electronic communication enters that information system; or

(ii) in any other case, at the time the electronic communication comes to the attention of the addressee.

B1.3 s221 When integrity of information maintained

(a) For the purposes of this subpart, the integrity of information is maintained only if the information has remained complete and unaltered, except for the addition of any endorsement, or any immaterial change, that arises in the normal course of communication, storage, or display.

B1.4 s228 Presumption about reliability of electronic signatures

(a) For the purposes of sections 226 and 227, it is presumed that an electronic signature is as reliable as is appropriate if:

(i) the means of creating the electronic signature is linked to the signatory and to no other person; and

(ii) the means of creating the electronic signature was under the control of the signatory and of no other person; and

(iii) any alteration to the electronic signature made after the time of signing is detectable; and

(iv) where the purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.

[1] Contract and Commercial Law Act 2017 http://www.legislation.govt.nz/act/public/2017/0005/21.0/whole.html.

B1.5 s222 Legal requirement that information be in writing

(a) A legal requirement that information be in writing is met by information that is in electronic form if the information is readily accessible so as to be usable for subsequent reference.

B1.6 s226 Legal requirement for signature

(a) A legal requirement for a signature other than a witness's signature is met by means of an electronic signature if the electronic signature:

(i) adequately identifies the signatory and adequately indicates the signatory's approval of the information to which the signature relates; and

(ii) is as reliable as is appropriate given the purpose for which, and the circumstances in which, the signature is required.

(b) However, a legal requirement for a signature that relates to information legally required to be given to a person is met by means of an electronic signature only if that person consents to receiving the electronic signature.

B1.7 s231 Extra conditions for electronic communications

(a) In addition to the conditions specified in section 230, if a person is required to retain information that is contained in an electronic communication:

(i) the person must also retain such information obtained by that person as enables the identification of

- the origin of the electronic communication; and
- the destination of the electronic communication; and
- the time when the electronic communication was sent and the time when it was received; and

(ii) the information referred to in paragraph (a) must be readily accessible so as to be usable for subsequent reference.

B1.8 Considerations

(a) **Time of dispatch and receipt.** If applicable, participants should address accessibility issues associated with certifying personnel working in remote locations out of cell coverage. This is particularly important for maintenance activities where there is a possibility that a certifier may certify maintenance and submit it, but the submission may not enter the proposed system until the mobile device is again within cell coverage. This means the certification would not be valid until it was received by the system. Should the aircraft be involved in an incident or accident prior to receipt, then there is the potential for the record to be lost. This situation is similar to the current situation with the CAA400, so participants should address it in their exposition and explain the equivalent level of accountability and safety.

(b) **Integrity of information.** Participants must demonstrate that their proposed system can guarantee that data in their systems is safe and cannot be altered. Relevant questions in this regard include:

(i) What data integrity/validation protocols exist to ensure a certified or signed document is not altered:

- without their knowing; and
- without an original being held available?

(ii) This requirement relates to both the signature itself and the data that the signature validates.

(c) **Legal requirement for signature and presumption of its reliability.** Participants must demonstrate that each signature entered is an accurate depiction of the known signature for that person. Relevant questions in this regard include:

(i) How does the operator adequately identify the signatory and adequately indicate the signatory’s approval or verification of the information to which the signature relates?

(ii) Is the system reliable with respect to the purpose and circumstances in which the signature is given?

(iii) How accurate and repeatable are signatures when all users sign using touchscreens?

(iv) If the software is utilising a different method of identity validation, such as RealMe, smart phone thumb prints, facial or voice recognition, the participant must outline how their system interfaces with the identity validation method.

(v) Are these media then acceptable for RTS purposes?

(vi) Is the appropriate RTS statement affixed next to the signature in their product?

NOTE: *Certain manufacturers prohibit maintenance records for their products being delivered in digital form. It is the operator’s responsibility to determine their obligations to all business stakeholders prior to considering the use of such products.*

NOTE: *When utilising external validation systems, care must be given to ensure that those validation systems comply with the relevant provisions in the Electronic Identity Verification Act 2012. This Act provides guidance on how an electronic identity that is held by an organisation may be used. Participants should also demonstrate some awareness of the robustness of validation systems from external companies or suppliers. For example, certain smartphone manufacturers publish promotional material on their websites regarding the security of various access methods (for example fingerprint signatures versus 4-digit PINs). Participants need to assess the best method for their operation.*

(d) **Requirement for information to be in writing.** Participants must demonstrate that the search function of their product is sufficient to ensure that all information is made available for search and validation in the future. Relevant questions in this regard include:

(i) How is the information presented for review as a comprehensive list and not just what the internal search algorithm in the software presents for review?

(ii) How do they access this information in the future for audit purposes?

(iii) How is access provided to external auditors like CAA? Is it permanent access or only for a limited period prior to audit?

(iv) Is it able to be quarantined in case of an accident?

(v) How does the maintenance controller and/or contractor review any pilot maintenance records each maintenance check to ensure they are complete? This information is required to be summarised in the logbook at each scheduled inspection.

(e) **Record keeping of electronic documents.** Participants must demonstrate how their record keeping procedures comply with the requirements of CCLA Section 231. This includes ensuring that all records stored in their databases are stamped with the metadata information. Note that Sections 215 and 216 of the CCLA define origin and destination of electronic transmissions.