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

Advisory Circular AC00-6

Revision 2

5 April 2025

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.

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 Law Act 2017 (CCLA 2017). 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

Revision 2 updates this AC in line with redrafted rules under the Civil Aviation Act 2023 (CA Act 2023). It also:

- adds an Introduction
- cuts duplicate sections
- amends Appendix B by removing specific quoted sections of the CCLA Act 2017 and replacing with a summary and website links, and
- makes formatting and stylistic updates to align with current AC format.

Version History

History Log.

Revision No.	Effective Date	Summary of Changes
AC00-6, Rev 0	20 July 2020	The initial issue of this AC.
AC00-6, Rev 0.1	7 April 2021	Removed a duplicate entry in the Definitions section
AC00-6, Rev 1	10 August 2022	Corrected an inaccurate reference to AC43-1, in Appendix A, p 17.
AC00-6, Rev 2	5 April 2025	Updates to align AC with redrafted rules under the CA Act 2023. Adds an Introduction section. Cuts duplicate sections Amends Appendix B by removing specific quoted sections of CCLA 2017 and replacing with a summary and website links Makes formatting and stylistic updates to align with current AC format.

Table of Contents

1. Introduction

As aircraft design, certification, operations and maintenance processes have become more complex, the number of records and documents generated and required by aircraft operators, manufacturers and approved maintenance organisations has increased.

Electronic information storage and retrieval systems have made it easier for the aviation industry to comply with their regulatory requirements and to compile and maintain records of highly complex aircraft and aircraft systems.

Electronic certifications and signatures, logbooks (chronological compliance records) and programmes/controls (e.g. computer software programmes or tablet / phone apps) containing navigation charts and weight and balance calculators are widely used in the industry.

Handwritten signatures can be illegible and paper documentation wears out over time, which is not the case for electronic signatures. However, electronic records also have vulnerabilities, e.g. if they are corrupted, or not stored or backed up securely. For electronic records to be acceptable, they must have processes in place to verify and store them, and personnel who are trained to manage these processes. These are explained in this AC.

No matter what system is used, records of electronic certifications and signatures need to be kept in an easily accessible form, so that operations specifications and other information can be assessed if required. These documents also form an important part of the reference material for other operations tasks, staff training, and continued operator responsibilities. Therefore, organisations need systems that ensure information security, integrity, and easy retrieval by people who need to access them.

***Note**: The CASA AC, AC 11-03 v3.0 - Electronically formatted certifications, records and management systems, also has useful guidance.*

2. Definitions

Definitions	
Authentication	the way a system validates the identity of an authorised user. This may include a password, a personal identification number (PIN), a cryptographic key, or smart card. They 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	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	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	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	a process of ensuring accuracy of data records by systematically or randomly comparing electronic records with manual data entry documents.

Digital Signature	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	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 manuals	aviation document holder manuals that may be electronically signed, stored, and retrieved by a computer system via CD-ROM, an app, internet/intranet-based files, or other forms of electronic media, including commercial off-the-shelf (COTS) portable electronic device (PED) hardware (for example laptop, tablet, phone).
Electronic record	contract or other record created, generated, sent, communicated, received, or stored by electronic means.
Electronic record keeping system	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	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) in the form of a document, a signature, a seal, data, text, images, sound, or speech.
Information system	a system for producing, sending, receiving, storing, displaying, or otherwise processing electronic communications.
Password	an identification code or device required to access stored material, intended to prevent information from being viewed, edited, or printed by unauthorised persons.
Signature	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.

3. Approval, acceptance, and authorisation

3.1 There are many civil aviation rules that address signatures, records/record keeping, and manuals. Appendix A lists rules that are impacted by electronic signatures and data storage systems. It is strongly recommended that a participant explains in its exposition how it uses and keeps records of these signatures and systems to ensure it complies with the relevant rules.

3.2 The information in this AC relates only to CAA's acceptance guidelines for electronic signature, electronic record keeping, and electronic manual systems/programs, as CAA does not have its own regulations for these. Any policy on electronic signatures and data storage systems must also comply with Part 4 of the CCLA 2017, which are summarised in Appendix B of this AC.

3.3 Each aviation business has its own unique framework of legislative responsibility and certain manufacturers prohibit the maintenance records for their products being delivered in digital form. Therefore it is the participant's responsibility to determine their obligations to all

business stakeholders, before using 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 in this AC are met. Applicants should be ensuring that their proposed hat their

3.2 Participants may also need to make sure that any electronic tools they want to use, meet all relevant legal and regulatory requirements, not just the ones in this AC. For example, where participants are applying for Electronic Flight Bag (EFB) programme approval using the advice in AC91-20, *Guidelines for the Approval and Use of Electronic Flight Bag Devices*, and their EFB programme includes functions and/or aspects that are in scope of AC-006, they may include in their application evidence that they are meeting acceptable means of compliance as outlined in:

(a) AC91-20, for functions that are covered in that AC, and

(b) AC00-6, for functions that are covered in that AC.

This will make it clear that the EFB programme, once approved, meets both the technical requirements of Part 91 and requirements relating to electronic signatures.

4 Electronic signatures

4.1 **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.

4.2 **Types of Electronic Signatures.** Electronic signatures may appear in various formats and must meet the requirements in Section 3, above. Examples of electronic signature formats include, but are not limited to:

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

(b) A digital signature

(c) A typed notation

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

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

(f) Any other acceptable form of individual identification that can be reliably used to verify a record, record entry or document.

Note: *Not all identifying information found in an electronic signature constitutes a signature, e.g. the entry of a person's name in an electronic system.*

4.3 **Electronic Signature Standards**. Electronic signatures should meet the following criteria to be considered legally binding:

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

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

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

(d) 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.

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

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

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

(h) 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).

4.4 **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 use 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.

4.5 **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:

(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. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. These could be encoded onto badges, cards, cryptographic keys, or other objects.

(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.

4.6 **Policies and Procedures.** An organisation's electronic signature policies and procedures should include information on:

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

(b) ***Authorised persons – security and access***. This should include 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. These 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 to Section 6 below for additional considerations.

(g) ***Computer System Outages and/or Disaster Recovery.*** Policy and procedures should address computer system outages (failure of hardware, software, application, network, etc.) and 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.

5 Electronic record keeping

5.1 **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, and /or

(e) drawings.

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

(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., crew member, 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.

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

(a) protect confidential information.

(b) ensure that the information in an electronic record is not altered in an unauthorised way.

(c) provide for secure access and contain safeguards against unauthorised access.

5.1 Participants also need to consider methods for:

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

(b) ***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.

(c) ***Ensuring 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, or an existing electronic system to a new electronic system.

(d) ***Ensuring Continuity of Records for Maintenance Providers.*** Procedures should ensure continuity with maintenance providers. Participants 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. They should include procedures for making required records available to CAA in a format and manner that is acceptable to CAA.

6 Electronic manual systems

6.1 **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:

(a) the manual title

(b) revision control pages or sections from which the user can readily determine whether the manual is current

(c) list of effective pages, in cases where individual pages are amended without a complete re-issue of the manual

(d) indication of CAA approval (e.g., signature or stamp) for those manuals or manual sections that require CAA approval

(e) chapter numbers and headings

(f) section numbers

(g) topic headings

(h) page numbers, if manuals are intended for distribution in hard copy format

(i) applicable aircraft, airframe, engine, propeller, appliance, component, or part make and model (when applicable for minimum equipment list (MEL) and maintenance purposes), and

(j) details of the person or team with the authority and responsibility for manual content.

6.2 **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) ***Minimum Equipment List (MEL).*** A means to provide flight crew with a MEL through printed or other means approved by CAA. An EFB is an example of other means that may be approved by CAA. Refer to AC91-20, *Guidelines for the Approval and Use of Electronic Flight Bag Devices,*

(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, or existing electronic system to a new 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, but also leave a clear record of revisions that have been made. The electronic manual system should include revision control procedures for making revisions (incremental, temporary, and scheduled) in a timely manner. Procedures should include how personnel should make and record revisions and who is authorised to do this. The revision control procedures should address at least:

(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 enable the user 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.

(i) ***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.

(j) ***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.

(k) ***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.

(l) ***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) Archived historical data is particularly important, among other 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) 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 for:

- ensuring that no unauthorised changes can be made.
- minimising the deterioration of data.
- protecting the archived data against hazards and natural disasters.

(m) Electronic master manuals must include at least:

(i) A description of the Electronic Manual System, including the methods for distribution and/or access to manual(s) (including manual revisions and replacements) by the appropriate personnel.

(ii) Delivery Media, including 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.'

7 Civil Aviation Rules – retention of records

The 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 affected rules are included in the tables below.

(b) 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, *Miscellaneous Rules*

Rule 19.321(b)(5) Supply control procedures	Release notes that are issued must be certified by an appropriately authorised person who is listed in the supply organisation's exposition. It would be good practice for an organisation to include an explanation of who is authorised to certify release notes and how this process is managed in their exposition.

A1.2 Part 43, *General Maintenance Rules*

Rule 43.69(a) and (b) Maintenance records	Rule requires use of 'appropriate' maintenance logbooks and associated worksheets. AC43-1, *Aircraft Maintenance,* para 2.14, explains the minimum requirements for maintenance records. If electronic records are used in place of CAA logbooks and worksheets, the entries into the electronic system must continue to satisfy the requirements of rule 43.69. The use of electronic records in place of CAA logbooks and/or worksheets, must be approved by the Director. Participants who want to use these methods, such as files or cloud storage, need to be able to explain to CAA how these records will be stored, and kept secure and as a permanent record.
Rule 43.69(d)(2) Maintenance records	A signature is required to certify a record of maintenance, **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 rule 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	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 rule 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	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 rule 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	For components defined in, rule 43.54 or exported by, Part 145, or Part 148-certificated organisations, a signature is required to certify RTS on a Form One. If Form Ones are to be in digital form, this record keeping system needs to be accepted by the Director, as outlined in rules 145.67(c) and 148.67(b).
Rule 43.105(b)(2) Certifying release-to-service after maintenance	For components that aren't fitted to aircraft, a signature is required to certify RTS on a Form Two. If Form Twos are to be in digital form, this record keeping system needs to be accepted by the Director, as outlined in rule 43.69(a) and (b).
Rule 43.109(3)(i) Defects	Any defects that remain un-cleared after maintenance checks are entered into the logbooks and/or technical log, need a signature to certify that the aircraft is *not* released to service. Refer to rule 43.69(a)(b) and (c).
Rule 43.113(d)(2) Duplicate safety inspection control system	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 this record keeping system needs to be accepted by the Director, as outlined in rule 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	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 this record keeping system needs to be accepted by the Director, as outlined in rule 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 rule 91.605(a)(3) and requires Director's approval of Part 119 maintenance programmes.
Rule 91.607(b) Approval of maintenance	Gives requirements for maintenance programmes that are to be approved under rule 91.607(a). Any electronic record keeping process that is outlined in this paragraph is then subject to approval by the Director.

programmes	
Rule 91.616(1) Maintenance logbooks	Requires 'appropriate' logbooks to be provided. Refer to rule 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 rule 91.617(a)(b) and (c), which refer to the record keeping systems in rule 43.69. Thus, this 'encoded' form of record keeping must be accepted by the Director. Refer to rule 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 Part 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 rule 91.617(a) and (b) must be transferred with aircraft ownership. This impacts on the requirements of any signature bearing record keeping systems that are accepted by the Director, under rule 43.69(a) and (b).
Rule 91.623 Retention of records	States all maintenance records must be retained for specified periods. This impacts on the requirements of any signature bearing record keeping systems that are accepted by the Director, under rule 43.69(a) and (b).

A1.4 Part 100, *Safety Management*

Rule 100.3(b) System for safety management	The organisation must document all processes required to establish and maintain the system for safety management (SMS). For more detail, refer to AC100-1, *Safety Management.* While Part 100 does not include details on record-keeping and electronic signatures, AC100-1, *Safety Management*, covers record-keeping in more detail. Electronic records and signature are not specifically ruled out, but, as an SMS has to be accepted by the Director, organisations need to be able to show how they will be able to safeguard the accuracy of their SMS records and sign-offs.

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	An airline operator must establish who has responsibility for oversight and maintenance of the system and include information about this as part of the exposition.
Rule 119.81(a) and (b) Airline air operator exposition	An airline operator's exposition must contain all information required by Part 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	A General Aviation Air Operator must establish who has responsibility for oversight and maintenance of the system and submit this information as part of the exposition.
Rule 119.125(a) and (b) General aviation air operator exposition	A General Aviation Air Operator's exposition must contain all the information required by Part 119 (including a maintenance programme that includes a description of the system used to record maintenance activity and retain those records). The exposition must be acceptable to the Director.
Rule 119.151(b)(ii) Continued compliance	A holder of an air operator certificate must comply with all the procedures and programmes in its exposition and make at least one copy of the relevant sections available to all staff that need it.

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

Rule 135.415(c) Maintenance review	Continuous maintenance review systems that form part of airline maintenance programmes need to be acceptable to the Director.
Rule 135.415(d)(3) Maintenance review	Signatures must be affixed to maintenance reviews for those carried out under the privileges of a Part 135 certificate. If these are certified electronically, these systems must form part of an exposition that is acceptable to the Director, under Part 119.
Rule 135.803(a)(4) Operator responsibilities	A Part 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 Part 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 Part 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 Part 119.
Rule 135.859(d) Retention period	Document retention requirements for daily flight records. Any electronic application used to record, track or advise personnel must also be acceptable to the Director and forms part of the certification requirements in Part 119.

A1.7 Part 141, *Aviation Training Organisations Certification*

Rule 141.63(b) Standard aviation training organisation exposition	An exposition must contain all information required by rule 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 to rule 119.321(b)(5).
Rule 145.55(2) Equipment, tools, and material	An 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, details of how this system will carry out these functions must be documented in the exposition. Refer to rule 145.67(c).
Rule 145.59(b)(6) and (7) Maintenance control procedures	An applicant must develop procedures for RTS of aircraft or components and to issue authorisations for certification of a Form One. If these are handled in electronic form, this must be documented in the exposition. Refer to rules 145.67(c) and 43.105(b)(1).
Rule 145.63(a) Records	An applicant must establish procedures for management of records to ensure a product or component is fit for RTS. If these are handled in electronic form, this must be documented in the exposition. Refer to rule 145.67(c).
Rule 145.67(a)(8)(vii), (x) and (xv) Maintenance organisation exposition	An exposition must contain procedures for performance of maintenance activities, RTS 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	An exposition must be acceptable to the Director.

A1.9 Part 146, *Aircraft Design Organisations Certification*

Rule 146.55(2) Equipment, tools, and data	An 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, details of how this system will carry out these functions must be documented in the exposition. Refer to rule 146.67(b).
Rule 146.59(b)(5)	An applicant must develop procedures for issuing statements of

and (6) Design control procedures	compliance and design change approvals. If these are handled and certified in electronic form, this must be documented in the exposition. Refer to rule 146.67(b).
Rule 146.63(a) Records	An applicant must 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 to rule 146.67(b).
Rule 146.67(b) Design organisation exposition	An exposition must be acceptable to the Director.

A1.10 Part 148, *Aircraft Manufacturing Organisations Certification*

Rule 148.55(2) Equipment, tools, and material	An 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, details of how this system will carry out these functions must be documented in the exposition. Refer to rule 148.67(b).
Rule 148.59(b)(7) Production control procedures	An applicant must develop procedures for issuing CAA Form One release certificates. If these are handled and certified in electronic form, this must be documented in the exposition. Refer to rule 148.67(b).
Rule 148.63(a) Records	An applicant must 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 to rule 148.67(b).
Rule 148.67(b) Manufacturing organisation exposition	An exposition must be acceptable to the Director.

APPENDIX B: Contract and Commercial Law Act 2017 (CCLA 2017), Part 4, Electronic Transactions - Summary of key provisions

Part 4 relates to electronic transactions, including matters relating to:

(a) improving certainty in relation to electronic information and electronic communications (see subpart 2):

(b) how legal requirements apply to electronic transactions (for example, requirements to give information in writing and to provide access to information) (see subpart 3)

The Act is available here: Contract and Commercial Law Act 2017 No 5 (as of 23 December 2023), Public Act – New Zealand Legislation. The relevant clauses are sections 213; 214; 221; 222; 226; 228 and 231.