Bermuda Advisory Circular BAC-AW-04	Issue: 1 Effective: 9-Jan-17
ACCEPTANCE OF ELECTRONIC MAINTENANCE RECORDS	

GENERAL

Bermuda Advisory Circulars are issued to provide advice, guidance and information on standards, practices and procedures necessary to support Overseas Territory Aviation Requirements (OTARS).

PURPOSE

This Bermuda Advisory Circular provides guidance on the acceptance and use of electronic aircraft maintenance recordkeeping systems (EAMR) which may also include the use of electronic signatures, as defined in appendix A of this Advisory Circular.

The guidance in this Advisory Circular pertains to an aircraft operator, an Aircraft Maintenance Organization, or a Continued Airworthiness Management Organisation here in after referred to as an Organisation.

RELATED REQUIREMENTS

This Circular relates to:

- OTAR Part 39 Continued Airworthiness Requirements
- OTAR Part 43 General Maintenance Requirements
- OTAR Part 145 Aircraft Maintenance Organisation Approval

CHANGE INFORMATION

This is the first issue of this Circular.

ENQUIRIES

Enquiries regarding the content of this Circular should be addressed to the Bermuda Civil Aviation Authority. Enquiries can be sent by email to info@bcaa.bm

Table of Contents

1 GENERAL

1.1 An electronic aircraft maintenance recordkeeping system (EAMR) is a system of record processing in which aircraft maintenance records are entered, stored, generated and retrieved electronically by a computer system rather than in the traditional hard copy paper form.

1.2 OTAR 39.73(d), 39.75, 43.57(c) and 145.117(c) concerning Maintenance records, requires an Organisation to make provision for the recording and retention of aircraft, engine and propeller maintenance records in hard copy or in electronic coded form. In the case where an Organisation chooses to develop and adopt an EAMR for the recording and retention of aircraft records in electronic coded form, the system shall have suitable backup and storage capabilities, security measures and safeguards, as outlined in this Advisory Circular. The guidance in this Advisory Circular provides an Organisation a method in which he can produce an EAMR system acceptable to the Governor.

1.3 EAMR systems can be separated into two distinct types.

(a) An EAMR system that enters, stores, generates and retrieves aircraft maintenance records electronically and incorporates the use of an electronic signature in the process. The requirements for this kind of EAMR are detailed in **Part A** of this Advisory Circular.

(b) An EAMR system that stores and retrieves aircraft records electronically but does not generate the original record. For example, in the case where aircraft maintenance records are originally in paper format and are scanned and filed electronically. The requirements for this kind of EAMR are detailed in **Part B** of this Advisory Circular.

1.4 Appendix B (EAMR REQUIREMENTS CHECKLIST) of this Advisory Circular should be used as a guide when developing an EAMR and procedures for the system.

1.5 The EAMR REQUIREMENTS CHECKLIST should be completed and form part of the EAMR procedures and be made available for review if requested by the BCAA.

2 APPLICABILITY

2.1 Any Organisation intending to utilize an EAMR system.

3 PART A

3.1 When constructing an EAMR to meet the maintenance records requirements in OTAR 39.73(d), 39.75, 43.57(c) and 145.117 (c) the following elements must be considered and addressed in the Organisation's procedures for the system:

(a) General Description. A general description of an EAMR system should be included in the procedures detailing but not limited to the following elements:

i. The computer software and hardware being used.

ii. Identify the users of the EAMR and describe the system access levels that are incorporated. For example, level one might be read only, level 2 read and enter and so on.

iii. Identify who retains ownership and responsibility for the EAMR and associated procedures.

iv. A flow process which describes generally how a maintenance record is entered, stored, generated and retrieved from the system.

(b) Security.

i. The electronic system should protect confidential information.

ii. The system should ensure that the information is not altered in an unauthorized way and should include data alteration traceability features.

iii. A corresponding policy and management structure should support the computer hardware and computer software that delivers the information.

(c) Procedures. Before introducing an electronic maintenance recordkeeping system, computer procedures must be developed to include the following:

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

ii. Procedures describing how electronic signatures will be used as it relates to all the elements that are associated with the use of electronic signatures, as detailed in Appendix A.

iii. Procedures to generate passwords and personal identification codes that ensure that the system will not permit password duplication.

iv. Procedures for auditing the computer system to ensure the integrity of the system. A record of the audit should be completed and retained on file in accordance with an Organisation's record retention policy. This audit may be a computer program that automatically audits itself.

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

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

vii. Procedures for EAMR backup for data loss and recovery.

viii. A description of the training procedure and requirements necessary to authorize access to the EAMR computer hardware and software system.

4 PART B

4.1 Procedures should be developed that consider those same elements previously mentioned in Part A of this Advisory Circular where applicable and are relative to the system size and complexity. The procedures should also include the Organisation's policy with regards to the disposition of any original hard copy maintenance records once they are entered into the EAMR.

APPENDIX A: ELECTRONIC SIGNATURE

Before the use of electronic signatures, handwritten signatures were used on any required record, record entry, or document to authentify it. The electronic signature's purpose is identical to that of a handwritten signature. The handwritten signature is universally accepted because it has certain qualities and features that should be preserved in any electronic signature. Therefore, an electronic signature should possess those qualities and attributes that guarantee a handwritten signature's authenticity.

DEFINITIONS

Digital Signature. Cryptographically generated data that identifies a document's signatory (signer) and certifies that the document has not been altered. Digital signature technology is the foundation of a variety of security, electronic business, and electronic commerce products. This technology is based on public/private key cryptography, digital signature technology used in secure messaging, public key infrastructure (PKI), virtual private network (VPN), web standards for secure transactions, and electronic digital signatures.

Electronic Signature. The online equivalent of a handwritten signature. It is an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by an individual. It electronically identifies and authenticates an individual entering, verifying, or auditing computer-based records. An electronic signature combines cryptographic functions of digital signatures with the image of an individual's handwritten signature or some other visible mark considered acceptable in a traditional signing process. It authenticates data with a hash algorithm and provides permanent, secure user-authentication.

In this Advisory Circular, the term "electronic signature" refers to either electronic signatures or digital signatures. The specific electronic signature used depends on the end user's preference and the system application.

An electronic signature may be part of an EAMR system and if so should consider the following:

(a) Uniqueness. An electronic signature should retain those qualities of a handwritten signature that guarantee its uniqueness. A signature should identify a specific individual and be difficult to duplicate. A unique signature provides evidence that an individual agrees with a statement. An electronic system cannot provide a unique identification with reasonable certainty unless the identification is difficult for an unauthorized individual to duplicate. An acceptable method of proving the uniqueness of a signature is by using an identification and authentication procedure that validates the identity of the signatory. For example, an individual using an electronic signature should be required to identify himself or herself, and the system that produces the electronic signature should then authenticate that identification. Acceptable means of identification and authentication include the use of separate and unrelated identification and authentication codes. These codes could be encoded onto badges, cards, cryptographic keys, or other objects. Systems using PINs or passwords also are an acceptable method of ensuring uniqueness. Additionally, a system could use

physical characteristics, such as a fingerprint, handprint, or voice pattern, as a method of identification and authorization.

(b) Scope. The scope of information being affirmed with an electronic signature should be clear to the signatory and to subsequent readers of the record, record entry, or document.

(c) Signature Security. The security of an individual's handwritten signature is maintained by ensuring that it is difficult for another individual to duplicate or alter it. An electronic signature should maintain an equivalent level of security. An electronic system that produces signatures should restrict other individuals from affixing another individual's signature to a record, record entry, or document. Such a system enhances safety by preventing an unauthorized individual from certifying required documents, such as an airworthiness release, and should include:

i. A corresponding policy and management structure must support the computer hardware and software that delivers the information.

ii. Signature authenticity/verification. Through control and archives, the computer software should determine if the signature is genuine and if the individual is authorized to participate. This can be accomplished by comparing the signature to a public key archive or some other means. This capability should be an integral part of the computer software.

iii. Archiving electronically signed documents: 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. This will provide for future authentication.

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

v. Procedures should be established allowing the organization to correct documents.

(d) Non-repudiation. An electronic signature should prevent a signatory from denying that he or she affixed a signature to a specific record, record entry, or document. The more difficult it is to duplicate a signature, the likelier the signature was created by the signatory.

(e) Traceability. An electronic signature should provide positive traceability to the individual who signed a record, record entry, or any other document.

Appendix B (EAMR REQUIREMENTS CHECKLIST)

BAC Reference	Requirement	Yes	No	Manual Ref
3.1 (a) General Description	**(1)** The computer software and hardware being used.			
	(2) Identify the users of the EAMR and describe the system access levels that are incorporated. For example, level one might be read only, level 2 read and enter and so on.			
	(3) Identify who retains ownership and responsibility for the EAMR and associated procedures.			
	(4) A flow process which describes generally how a maintenance record is entered, stored, generated and retrieved from the system.			
3.1 (b) Security	**(1)** The electronic system should protect confidential information			
	(2) The system should ensure that the information is not altered in an unauthorized way and should include data alteration traceability features.			
	(3) A corresponding policy and management structure should support the computer hardware and computer software that delivers the information.			

BAC Reference	Requirement	Yes	No	Manual Ref
3.1 (c) Procedures	**(1)** Procedures for making maintenance records available for review by the BCAA. This procedure and computer system must be capable of producing paper copies of the viewed information at the request of the BCAA.			
	(2) Procedures describing how electronic signatures will be used as it relates to all the elements that are associated with the use of electronic signatures, as detailed in Appendix A.			
	(3) Procedures to generate passwords and personal identification codes that ensure that the system will not permit password duplication.			
	(4) Procedures for auditing the computer system to ensure the integrity of the system. A record of the audit should be completed and retained on file in accordance with the Organisation's record retention policy. This audit may be a computer program that automatically audits itself.			
	(5) Procedures describing how the Organisation will ensure that the computerized records are transmitted in accordance with the appropriate regulatory requirements to customers or to another Organisation. The records may be either electronic or paper copies.			
	(6) Procedures to ensure that records required to be transferred with an aircraft are in a format (either electronic or on paper) that is acceptable to the new owner/operator.			
	(7) Procedures for EAMR backup for data loss and recovery.			
	(8) A description of the training procedure and requirements necessary to authorize access to the EAMR computer hardware and software system.			