Circular No.6-018

General Standards for Electronic Signatures and Electronic Records

Revision History

March 29, 2019 First issue

Airworthiness Division, Aviation Safety and Security Department
Japan Civil Aviation Bureau
Ministry of Land, Infrastructure, Transport and Tourism

(translated on June 4, 2019)

Circular No.6-018

March 29, 2019: First issue (KOKU-KU-KOU-2933, KOKU-KU-KI-1692)

Flight Standards Division /Airworthiness Division
Aviation Safety and Security Department
Japan Civil Aviation Bureau
Ministry of Land, Infrastructure, Transport and Tourism

Title: General Standards for Electronic Signatures and Electronic Records

Chapter 1 General Provisions

1.1 Purpose

This Circular provides for the details of the standards applicable in any cases where a flight logbook or any other documents, which must be kept under the Civil Aeronautics Law (Act No.231 of 1952) or related regulations, is handled by electronic measures in lieu of paper documents pursuant to the Regulation for Enforcement of the Act on Utilization of Telecommunications Technology in Document Preservation, etc. Conducted by Private Business Operators, etc. under the Jurisdiction of the Ministry of Land, Infrastructure, Transport and Tourism (Regulations of the Ministry of Land, Infrastructure, Transport and Tourism No.26 of 2005). The persons concerned are required to follow these General Standards, in principle.

1.2 Reference Documents

- FAA AC120-78A
- JIS Q 27001:2014

1.3 Definitions of terms

Definitions of terms used in this circular are as follows:

(1) Information system

An information system means a system consisting of hardware and software that is used for recording, processing and transmitting of information.

(2) Electronic signature

An electronic signature means that prescribed in Article 2, paragraph (1) of the Act on Electronic Signatures and Certification Business (Act No. 102 of 2000; hereinafter referred to as the "Electronic Signatures Act").

(3) Digital signature

A digital signature means one form of electronic signature that is based on encryption technology for recognition of the signatory which can be conducted only by the signatory him/herself in accordance with the relevant format.

(4) Electronic records

An electronic record means a record made in an electronic form, a magnetic form, or any other form not recognizable to human perception (hereinafter referred to as an "electronic measures") that is used in information processing by computers (pursuant to the provisions of Article 2, paragraph (4) of the Act on Utilization of Telecommunications Technology in Document Preservation, etc. Conducted by Private Business Operators, etc. (Act No.149 of 2004)).

(Note) This Circular applies to electronic records created by both of the following methods, irrespective of whether an electronic signature is required or not.

(i) A method of saving a created electronic record as a file prepared based on a file or magnetic disc stored in a computer used by a private business operators, etc. CD-ROM or other equivalent means which can surely record certain matters (when an original is created as an electronic record)

(ii) A method of saving an electronic record created by scanning matters written in a document (using a scanner or other equivalent image reading system) as a file prepared based on a file or magnetic disc, etc. stored in a computer used by a private business operators, etc. (when an original is created in paper and is saved in a computerized file in an electronic form)

(5) Archive

An archive means information that is properly maintained for the purpose of continued use within information created by work.

(6) Backup

A backup means using one of several recognized 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 recordkeeping system.

Chapter 2 Common Requirements for Electronic Signatures and Electronic Records

2.1 General

Electronic signatures and electronic records handled under the information system must conform to the requirements specified in the Civil Aeronautics Law, related regulations and Circulars, etc. (hereinafter referred to as "laws and regulations"), in addition to the requirements specified in this Circular.

2.2 Responsible personnel

The following persons must be appointed.

(1) A person who has the responsibility and authority in securing the integrity of the information system, managing the information security, and controlling access to the computer software.

(2) A person who has the responsibility and authority in establishing or revising the implementation manual specified in 2.13 below and ensuring that all users of the information system (including contractors) use the system in accordance with the prescribed procedures. The responsibility includes the dissemination of required duties among all users, and the management of education and training, etc.

(3) A person who has the responsibility and authority for information security measures required for the entirety of the life cycle of the information system, covering planning, development, operation and maintenance.

2.3 Identification of users of electronic signatures and electronic records

The information system must be one that can identify persons authorized to use electronic signatures or electronic records, purposes of use (retrieving, input, correction, authorization, etc.), and object records which are accessed.

(1) Access authorization

A means to grant the authority to access the information system to persons who need to create electronic records (including contractors) must be specified. Additionally, necessary authority must also be granted to the concerned authorities.

(2) Procedures for entering or retrieving data for the information system

Procedures to be followed by users of the information system for entering or retrieving data must be specified.

The information system must have a means to clearly distinguish authorized persons and unauthorized persons, and identify persons who are authorized to entering data (a means to issue an access code and password to validate data entry).

2.4 Validity of electronic records with electronic signatures

When using an electronic means for preparing and preserving any record for which affixing a signature or a name and seal is required under laws and regulations, the requirements specified in Chapter 3 must be satisfied.

2.5 Quality control

The information system must have a means to periodically audit its quality and integrity (the properties of being integral and accurate). This audit may be a self-test computer program that automatically audits itself.

If workstations are server-based and contain no inherent attributes that enable or disable access, there is no need for each workstation to be audited.

A records of the audit must be completed and retained on file.

2.6 Training and User Instructions

Instructions to be followed by users for entering, maintaining or retrieving data from the information system must be specified and training needs to be provided.

The training must include security awareness and information system integrity, as well as procedures that are necessary to authorize access to the information system. The procedures must include those for contractors that can directly access the information system as well as for the concerned authorities.

Additionally, a method of informing users of any changes in procedures, etc. must be specified.

2.7 Record transfer

When a user of an aircraft or aircraft part, etc. is changed or any aircraft or aircraft part, etc. is sold, records of the relevant aircraft or aircraft part, etc. must be transferred by ensuring with

satisfying the requirements under laws and regulations, together with the relevant aircraft or aircraft part, etc.

2.8 Continuity of data

Data of electronic signatures or electronic records must satisfy the following.

(1) Procedure must ensure the continuity of data in the process of transfer from a legacy (paper) system to an electronic system.
(2) When updating the information system or changing to a new system, the continued integrity must be ensured.
(3) When transferring data from legacy (paper) system to an electronic system, updating the information system, or changing to a new system, it is preferable to set a transitional period during which both systems may be utilized.

2.9 Continuity of Records for Contractors

When providing or receiving records to or from contractors, the quality and integrity of the records must be ensured.

(1) A method of receiving records from contractors and a method of transferring data to the originating company's information system must be clarified.
(2) When contractors directly input data into the originating company's information system, the originating company must manage access authority and clarify the permissible scope of data input by contractors.

2.10 System Support

(1) The hardware and software which constitute the information system, must be properly maintained.
(2) Alternate measures and data recovering measures for information system outage (failure of computer hardware, software or application network, etc.) or damages must be prepared.

2.11 Data Backup and Retention

Policy and procedures must address how data backup and retention of data will be accomplished.

(1) Data backup and retention are to be ensured.
(2) Methods of data retention and backup are robust and reliable.
(3) Timing and frequency of backups are appropriate for relevant records.
(4) Backed up data are isolated from the original data to prevent that the original and backup data are damaged simultaneously due to disaster.
(5) Backed up data are restorable when the original data are lost.

2.12 Auditing Process

An audit must be conducted periodically in order to ensure all the requirements continue to be met specified in this Circular.

An audit process must include measures concerning information security as well as actions to be taken to unauthorized events.

2.13 Policies and Procedures

When conducting electronic recordkeeping process or electronic signature process for record, policies and procedures must ensure following:

(1) Establishment or change of policies and procedures manual

Policies and procedures manual must be established based on the requirements specified in this Chapter, Chapter 3 and Chapter 4. When there has been a change in any matters specified in the manual, or when any actions to be taken are required as a result of an internal audit, manual must be reviewed and revised appropriately and must be managed to ensure that the manual satisfies the requirements specified in this Circular.

(2) Description of electronic recordkeeping and electronic signature process

The manual must contain the following matters.

(i) Outline of the information system (hardware and software, etc.) (Software versions must be identified.)

(ii) Types of electronic records for which electronic signatures are to be applied.

(iii) Types of electronic records that are to be retained in the information system

(3) Dissemination of Policies and Procedures manual

The policies and procedures manual must be kept available to all users and the content thereof must be made known to all users.

Chapter 3 Individual Requirements for Electronic Signatures

3.1 General

Electronic signatures must meet the requirements specified in Chapter 2 and this Chapter irrespective of their types (entering a user's name and password, using a digital signature, etc.).

An electronic signature by the signatory him/herself on an electronic record is deemed to have the same effect as a signature or a name and seal affixed on a written document. The Electronic Signatures Act provides as follows.

Chapter II Presumption of Authentic Establishment of Electromagnetic Record

Article 3 Any electromagnetic record that is made in order to express information (except for that prepared by a public official in the course of duties) shall be presumed to be established authentically if the Electronic Signature (limited to that which can be performed by the signatory through appropriate management of codes and properties necessary to perform this) is performed by the signatory with respect to information recorded in such electromagnetic record.

3.2 Authenticity

(1) An electronic signature is only valid if it is unique to the individual signatory. It must identify a specific individual and be difficult to duplicate.

(i) When the signatory performs an electronic signature, the valid electronic signature must be under the sole control of the signatory and the signatory must be identified with his/her specific data for accessing the information system (with his/her name and password, etc.).

(ii) An electronic signature must be difficult to duplicate.

(2) An electronic signature must be executed or adopted by the signatory with the intent to sign the electronic record to indicate a person’s approval or affirmation of the information contained in the electronic record.

(i) It must be clear to the signatory exactly what it is that he/her is signing.

(ii) A process must be established to ensure that the signatory is provided with an opportunity to check and understand the content of each record before performing an electronic signature and that electronic signatures are applied only to records whose content is understood by the signatory.

(iii) The signatory must perform an electronic signature based on his/her own will. Specific methods of presuming that an electronic signature is based on the signatory's will are as follows:

- a digitalized image of a hand-written signature is integrated into electronic record
- using an electronic pointing device
- entering a user's name and password
- swiping a badge using an ID card
- using biometric identification information (fingerprints, vocal patterns, the retina, etc.)
- using a digital signature

(3) The signatory needs to be notified of the completion of an electronic signature.

3.3 Integrity

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

(2) An electronic signature must remain valid during the guaranteed period.

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

(i) There must be a means to put in place to archive a record with an electronic signature safely while maintaining the validity of the electronic signature.

(ii) The archive must satisfy the retention period of the relevant record.

3.4 Confidentiality

(1) There must be a means to identify a specific individual as the signatory and conduct authorized access control.

(2) There must be a means to prevent unauthorized individuals from performing the electronic signatures.

3.5 Traceability

(1) The information with an electronic signature must unalterable without a new signature.

(2) An electronic signature process must include a means 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 a data is in error..

(3) An electronic signature must be invalidated any time a superseding entry is made to correct the record or document. The information or signature being corrected must be voided but remain in place.
(4) The new information and/or signature must be easily identifiable.

3.6 Undeniable

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.

3.7 Security

(1) A process of electronic signature must be robust.
(2) Unauthorized access to the information system needs to be prevented.
(3) The process must contain procedures to prohibit the use of an individual's electronic signature when the individual leaves or terminates employment.

Chapter 4 Individual Requirements for Electronic Records

4.1 General

The security of the information system must be maintained and electronic records must have the integrity, confidentiality and readability at the levels equivalent to or more than paper system.

4.2 Integrity

Electronic record system must have a means to protect against loss, destruction, tampering or deletion of the record.

4.3 Confidentiality

Electronic record system must protect confidential information and prevent access by unauthorized persons.

4.4 Readability

The electronic record system must have a means to display clearly on a screen legible as the paper records and to make paper copy as necessary. Additionally, it must be ensured that the signatory can identify records for which he/she performed electronic signatures and can retrieve the data.

Supplementary Provisions

1. This Circular shall be enforced on April 1, 2019.