Statutory Instrument No. of 2015

ELECTRONIC RECORDS (EVIDENCE) ACT

(No. 13 of 2014)

ELECTRONIC RECORDS (EVIDENCE) REGULATIONS

(Published on , 2015)

ARRANGEMENT OF REGULATIONS

REGULATION

IN EXERCISE of the powers conferred on the Minister of Defence, Justice and Security by section 16 of the Electronic Records (Evidence) Act, the following Regulations are hereby made -

Citation

1. These Regulations may be cited as the Electronic Records (Evidence) Regulations, 2015.

Interpretation

2. In these Regulations, unless the context otherwise requires -

"**applicant**" means the party who has applied to be certified as provided in regulation 3.

"**certification**" means the process of assessment and confirmation that a process constitutes an approved process, in accordance with the compliance criteria;

"**certifying authority**" means the Communications Regulatory Authority;

"**compliance criteria**" means the criteria set out in the First Schedule which is applied to a process for purposes of certification;

"document image" mean a representation of a document generated by photographic, electronic or other means, which is stored in the document imaging system;

"**document imaging system**" means any computer system that is capable of capturing, storing and retrieving digital images of physical documents.

Application for certification

3. An application for certification shall be made in such form as provided by the certifying authority and accompanied by-

(a) such documents and information as specified on form A ***(BOCRA to develop the form);***

(b) Application fee of P5000,00;

(c) such further documents or information as the certifying authority may require.

Compliance criteria

4. The certifying authority shall, before certifying a process or any part thereof as an approved process, satisfy itself that the process is in compliance with the compliance criteria set out in the First Schedule.

Types of certificates

5. (1) Where the certifying authority is satisfied that a process or any part of a process meets the compliance criteria, the certifying authority shall issue a certificate as specified in the Second Schedule.

(2) If a process or any part of a process does not meet all the requirements of the compliance criteria, the certifying authority may –

(a) issue a qualified certificate in accordance with the conditions specified in the Second Schedule; or

(b) refuse to certify the process.

Written representation

6. The certifying authority may obtain from any person who has provided information in the certification process, a written statement that-

(a) the person has not provided information which he or she knows or is reasonably expected to know to be false or does not reasonably believe to be true; and

(b) the person has not knowingly withheld information which he or she is reasonably expected to know is relevant to the certification.

Civil penalties

7. Any person who makes a false representation in the certification process shall be liable to a civil penalty not exceeding P5, 000 as the certifying authority may impose.

Exemption

8. If an electronic document produced by the applicant originates from an independent party, over which the applicant has no control, it is adequate for the certifying authority to certify the process of the applicant to receive, store and present the electronic document, without extending the work to cover the process of the originator.

FIRST SCHEDULE

(regulation 4)

COMPLIANCE CRITERIA FOR APPROVED PROCESS

Introduction

1. This Schedule sets out, for the purposes of section 6(1) of the Act, the compliance criteria applicable in the certification of an approved process.

2. When certifying an approved process, the certifying authority shall:

   (a) identify the electronic records system, including that part of the system that is relevant to the legal proceedings in question

   (b) satisfy itself regarding the controls surrounding and within that electronic records system that would ensure the integrity of the relevant electronic records (); and

   (c) identify the party responsible for the operations or management of the approved process ().

3. Controls for the purpose of paragraph 2 (b) above include but are not be limited to the following inter-dependent areas-

   (a) controls implemented as part of computer system security, which provides a controlled environment for electronic records to be preserved (Part I);

   (b) controls implemented as part of the application program that maintains the electronic records (Part II);

   (c) controls implemented as part of the business process that produces the electronic records (Part III);

   (d) controls implemented as part of document imaging process that converts physical documents into electronic form (Part IV);

   (e) controls for retrieving and preparing the electronic records for presentation as evidence (Part V); and

   (f) controls implemented using digital signature (Part VI).

4. The compliance criteria are listed in Parts I to V below. Each given criterion must be satisfied, as appropriate, through a combination of both the design of the control and operational effectiveness of the control, for the period the electronic record resides in the computer system.

5. If a given criteria cannot be satisfied through controls, then its risks have to be reasonably compensated by other criteria in this Schedule.

PART 1 - COMPUTER SYSTEM SECURITY

Objective

6. The objective of this Part is to provide a set of compliance criteria that will reasonably ensure that the electronic records in a computer system are secured and accessible .

Compliance criteria

7. The criteria in this Part are organised into two groups:

   (a) Information Technology processes (also commonly known as IT General Controls); and

   (b) Technical security.

Information Technology processes

8. Organisation structure and individual roles and responsibilities reasonably ensure that Information Technology controls are effectively enforced.

   Illustration of controls:

   (a) An independent and competent Information Technology function acts as the custodian and operates the computer system;

   (b) Security policies and procedures exist and are complied with; and

   (c) Segregation of duties is enforced within Information Technology to separate application development, security administration and production system operations.

9. Access to programs and data are authorised and monitored.

   Illustration of controls:

   (a) Physical access restrictions to system and terminals;

   (b) Controls are effective over provisioning, changing and removing of user Identity Document and access rights at system, database and application levels;

   (c) Controls are effective over activation and monitoring of emergency Identity Documents; and

   (d) Security audit logs are checked.

10. Changes to system configuration, application programs and data are authorised and monitored.
Illustration of controls:

    (a) Production environment is isolated and secured ;

    (b) Source codes of applications are secured or not accessible ;

    (c) Changes are approved, checked and tested; and

    (d) Audit trails are checked.

11. Computer operations are genuine and monitored.

    Illustration of controls:

    (a) Use of batch jobs is controlled; and

    (b) Backups used to ensure availability and accessibility of electronic records.

Technical security

12. Network has been secured to prevent unauthorised access to electronic records.

13. Computer system has been secured at the operating system level to prevent unauthorised access to electronic records.

14. Database has been secured to prevent unauthorised access to electronic records.

PART II – APPLICATION SYSTEM SECURITY

Objective

15. The objective of this Part is to provide a set of compliance criteria that will reasonably ensure that the electronic records in an application system are secured and accessible. Application system security can only be relied on if there is reasonable computer system security.

Compliance criteria

16. User access controls reasonably restrict users to functions appropriate to their job roles and enforce segregation of duties.

17. Input controls reasonably ensure the accuracy of data. Input controls would be relevant if the evidence presented is relating to data or interpretation of data.

18. Processing controls reasonably ensure the accuracy of information produced. Processing controls would be relevant if the evidence presented is automatically generated or has been processed by the application system.

19. Output controls reasonably ensure that the electronic records presented are what they are in the system.

Illustration of controls:

(a) Query and reports are produced based on correct parameters and logic; and

(b) Output is directly from the system and not subject to human interventions.

\PART III – BUSINESS PROCESS CONTROLS

Objective

20. The objective of this Part is to provide a set of compliance criteria that will reasonably ensure that the electronic records are genuine, complete, up-to-date and correct.

Compliance Criteria

21. Segregation of duties is designed to provide assurance that records are genuine and correct.

22. Maker and checker controls are used to ensure sensitive records are correct.

23. Reports checking and reconciliation controls ensure that information is correct.

PART IV – DOCUMENT IMAGING CONTROLS

Objective

24. The objective of this Part is to provide a set of compliance criteria that will reasonably ensure that electronic images of physical documents are correct representations of the physical documents.

Compliance criteria

25. The electronic images are produced in the normal course of business.

26. Quality control method is applied to the document imaging process to ensure that the electronic document images are correct representations of the original documents, and that the relevant metadata (such as document Identity Document, data and time) and indices are coded correctly.

27. The electronic images are protected against subsequent malicious alterations and deletions.

28. The metadata and indices that are relevant to the electronic images and used to ensure the correct retrieval of images are equally protected against malicious alterations and deletions.

29. There is a means to verify that the electronic document images have come from the document imaging process that complies with the criteria in this Part.

PART V – RETRIEVING AND PREPARING EVIDENCE

Objective

30. The objective of this Part is to provide a set of compliance criteria that will reasonably ensure that the electronic records produced as evidence come from the systems and processes that are the subject of the certification exercise.

Compliance criteria

31. The process for retrieving and preparing the evidence has been documented.

32. The retrieval and preparation process has been witnessed.

33. There is proof that the evidence is directly produced by the systems and processes.

PART VI – DIGITAL SIGNATURE

Objective

34. The use of digital signature can prove that an electronic document or record has not been modified since the time the digital signature is applied. The objective of this Part is to provide a set of compliance criteria that will reasonably verify that digital signature has been effectively applied.

Compliance criteria

35. The digital signature used is one that is reasonably appropriate considering the nature and risk of the electronic documents or records it is being applied to.

36. The secret keys used to generate the digital signature are reasonably secured and safe-guarded against unauthorised disclosure.

37. A process exists to reasonably ensure that the digital signature is applied to the electronic documents or records at a time of relevance.

38. A process exists and is used to verify the digital signature at the time of retrieval of the electronic documents or records.

SECOND SCHEDULE

(*regulation 5)*

TYPES OF CERTIFICATE

The following are the possible certificate conclusions that the certifying authority may use depending on their findings.

Type	Conditions
Unqualified	The certifying authority is satisfied that the electronic records met all compliance criteria
Unqualified with notes	The certifying authority is satisfied that the electronic records met all compliance criteria, but has comments for considerations and to be put on the records
Qualified	The certifying authority is generally satisfied that the electronic records have met *[all]* compliance criteria except in some specific areas that may affect the integrity of the electronic records
Qualified with serious constraints	The certifying authority noted areas of non-compliance or inability to verify compliance, which may cast doubt over the integrity of the electronic records
Abstained	The certifying authority was unable to verify that the compliance criteria have been met and would not testify to the integrity of the electronic records

THIRD SCHEDULE - FORMS

FORM A - Application Form

Made this of 2015

_____
SHAW KGATHI
Minister of Defence, Justice and Security