Draft
L.P.
10.11.15

Statutory Instrument No. of 2015

ELECTRONIC RECORDS (EVIDENCE) ACT
(ACT NO. 13 OF 2014)

ELECTRONIC RECORDS (EVIDENCE) REGULATIONS, 2015
(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 maybe be cited as the Electronic Records (Evidence) Regulations, 2015.

Interpretation

2. In these Regulations, unless the context otherwise provides –

"certifying authority" means the Communications Regulatory Authority established under section 3 of the Communications Regulatory Authority Act; and

Cap. 72:03

"compliance criteria" means the criteria set out in Schedule 2 which is applied to a

process for the purpose of certification.

Application for certification

3. A person who wishes to operate or manage an approved process shall make an application to the certifying authority in Form A set out in Schedule 1, accompanied by –

(a) an application fee of P5 000; and

(b) such other information as may be required by the certifying authority.

Compliance criteria

4. The certifying authority shall before certifying a process or any part thereof as an approved process or management of the process satisfy itself that the process is in compliance with the compliance criteria set out in Schedule 2.

Issuance of certificate

5. (1) The certifying authority shall issue a certificate as set out in Schedule 2, if it is satisfied that a process or management of the process meets the compliance criteria.

(2) If a process or any part of the 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 Schedule 2; or

(b) refuse to certify the process.

Revocation, suspension or cancellation

6. The certifying authority may revoke, cancel or suspend a certificate issued under regulation 5 where it is of the view that the information provided for approval of a process or management of the process does not comply with the compliance criteria set out in Schedule 2.

Representation

7. The certifying authority may obtain a written statement from any person who has provided information in the certification process, 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; or

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

Exemptions

8. Where an electronic document produced by an applicant originates from an independent party over which the applicant has no control, it shall be sufficient for a certifying authority to certify the process of the applicant to receive, store and present the electronic document.

Civil penalty

9. A 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.

SCHEDULES
SCHEDULE 1

FORM A
(regulation 3)

BOCRA

APPLICATION FORM FOR CERTIFICATION OF ELECTRONIC RECORD SYSTEMS

SECTION 1: PARTICULARS OF THE APPLICANT

1.1 Applicant's Details

Company Name:	
Physical Address:	
Postal address:	
Telephone:	
Facsimile:	
Mobile:	
Email:	

1.2 Contact Person Details (Official Communication)

Name:	
Designation:	
Physical Address:	
Postal Address:	
National I.D / Passport No:	

Telephone:	
Email Address	
Facsimile:	
Mobile:	
Email:	

1.3 Company Registration
State whether company is
Public Limited
Private Limited
Parastatal
Others (please specify

Main business activity	
Company website (URL)	

The following information should be attached:

i) Company registration certificate, where the applicant company is a subsidiary of another company, information about the parent and ultimate holding companies (the entire group structure) must be provided.

1.4 Ownership

Provide Names, addresses and contact details of Directors/ Board Members:

Name of Company/Individual	
Country of Incorporation/ Nationality	
National I.D/Passport No	
Physical Address	
Postal Address	
Share %	

Name of Company/Individual	
Country of Incorporation/ Nationality	
National I.D/Passport No	
Physical Address	
Postal Address	
Share %	

Please attach shareholder certificates

1.5 Organisational Structure

Provide the details of the key Personnel responsible for Information Technology Process

Name:		Name:	
Designation:		Designation:	
Responsibility:		Responsibility:	
Physical Address:		Physical Address:	
Postal Address:		Postal Address:	
National I.D / Passport No:		National I.D / Passport No:	
Telephone:	(Work) (Res)	Telephone:	(Work) (Res)
Facsimile:		Facsimile:	
Mobile:		Mobile:	
Email:		Email:	

Name:		Name:	
Designation:		Designation:	
Responsibility:		Responsibility:	
Physical Address:		Physical Address:	

Postal Address:		Postal Address:	
National I.D / Passport No:		National I.D / Passport No:	
Telephone:	(Work) (Res)	Telephone:	(Work) (Res)
Facsimile:		Facsimile:	
Mobile:		Mobile:	
Email:		Email:	

Organisational structure and individual roles and responsibility that ensure that Information Technology processes are effectively complied with should be provided and clearly explained. Provide the curriculum vitae for the key personnel.

SECTION 2: CERTIFICATION RECOGNITION

2.1 Has the electronic record system applied to a competent authority in another jurisdiction/country for certification for electronic evidence purposes?

.....

.....

If yes, please state the result and the name of the jurisdiction/country. If the application is unsuccessful, please provide the reasons and submit the compliance audit report

.....

.....

.....

.....

.....

2.2 If the Applicant was successful in that other jurisdiction/country, a copy of the certificate, compliance audit report, copy of the Electronic Records (Evidence) Act and Regulations must be provided.

.....

.....

SECTION 3: LEGAL PROCEEDINGS INFORMATION

3.1 Has the applicant electronic record system ever been involved in any legal proceeding or dispute settlement in Botswana or in another country in connection with electronic (records) evidence it produces?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate):

.....

.....

.....

.....

3.2 Has the applicant company or its substantial shareholder or any of their respective directors and key executives, or any of the trusted persons, ever been convicted of an offence for which the conviction involved a finding that it/he/she acted fraudulently or dishonestly?

Yes No

If the answer to the above question is "yes", please furnish complete details (please attach a separate sheet if the space provided is inadequate):

.....

.....

.....

SECTION 4: ANNEXURES

The Applicant should attach the following documents in relation to the proposed electronic record system for the certification:

i) Full technical description
ii) Computer System Security Controls
iii) Software Application Systems Security Controls

iv) Business Process Controls
v) Document Imaging Controls
vi) Retrieving and Output Controls
vii) Digital signature controls
viii) Operation and management controls
ix) Privacy/security policy
x) Human Resource plan including the organisational chart, CV of the key personnel
xi) Incident Management plans and Disaster Recovery Plan
xii) Audited Financial Report for the previous two years

SECTION 5: DECLARATION

1. In applying to the BOCRA to operate for the certification of the electronic record system under the Electronic Records (Evidence) Act and the Regulations, I declare that all the above information provided by the company is true and complete.

.....

2. In the event that any of the information provided by the company is found to be false or misleading, the BOCRA reserves the right to take appropriate enforcement action against the company under the Act and/or the Regulations (including, without limitation, cancelling or suspending the accreditation of the company).

Applicant Name:

Signature: _____
Designation

Date:

Company Stamp:

SCHEDULE 2

COMPLIANCE CRITERIA FOR APPROVED PROCESS
(regulation 4)

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 provide 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

1. 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

2. 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

3. 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.

4. 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.

5. 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.

6. 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

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

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

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

PART II – APPLICATION SYSTEM SECURITY

Objective

1. 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

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

3. 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.

4. 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.

5. 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

1. 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

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

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

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

PART IV – DOCUMENT IMAGING CONTROLS

Objective

1. 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

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

3. 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.

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

5. 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.

6. 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

1. 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

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

3. The retrieval and preparation process has been witnessed.

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

PART VI – SECURE ELECTRONIC SIGNATURE

Objective

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

Compliance criteria

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

3. The secret keys used to generate the secure electronic signature are reasonably secured and safe-guarded against unauthorised disclosure.

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

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

TYPES OF CERTIFICATES
(regulation 5)

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

MADE this of , 2015.

SHAW KGATHI
Minister of Defence, Justice and Security