WHITEPAPER

How to Store & Archive businesses email

The South African best-practise approach

Author: Web Tech Law Proprietary (Limited) for SYNAQ PTY (Ltd)
28.02.2013

Tel +27 11 262 3632 www.synaq.com info@synaq.com

SYNAQ

Email Archival Compliance

In order to keep you up to date with the law regarding **email archival** compliance, we've put together this handy document that offers guidelines in an easy to digest manner. There is legislation in place the Electronic Communications and Transactions Act, passed in 2002 - that suggests you need to keep certain electronic documents on hand for various periods of time. Adequate email retention systems are essential in an environment **where digital communications are prevalent**.

Digital records are now accepted as functional and legal data records, meaning that retention methods must be put in place to secure and accommodate them.

Summary of General Retention Trends in South Africa

The standard practice in South Africa is to **retain email for three years**. There are exceptions to this rule, such as a Companies Act whereby electronic documents may have to be retained for up to seven years. One of the primary reasons for **information to be retained is for evidentiary purposes**. Sections 14 and 15 of the Electronic Communications and Transactions Act deal with originality and admissibility and evidential weight of data messages, respectively.

There are no less than 26 laws that require businesses to retain certain records for periods ranging from 3 to 30 years, even if it's in email format. Here's a **checklist you can refer to when looking at retaining your emails** and electronic documents.

Email Retention Checklist

This retention and archival checklist **complies with the Electronic Communications and Transactions Act** and associated laws or legal frameworks.

- Emails must be captured and stored in their final form and must be capable of being displayed or presented in this form
- Emails must not be altered in any way
- The form in which the emails are stored must allow for them to be viewed to accurately showcase the information generated, sent or received in final form
- The email archival service must be able to verify and track the lifespan of stored emails as well as any actions taken which may affect the stored emails or their storage environment
- Information about the email origin must be ascertainable, retained and associated with the emails themselves either in a manner which is consistent with their final form or in a manner which does not undermine the email integrity
- Emails must be retained in such a manner that the information is accessible
- The email archival infrastructure must be subject to regular and verifiable checks in order to ensure integrity and proper functioning
- Emails must be capable of being extracted from their storage environment in a non-destructive manner to preserve the information extracted as evidence as well as the stored versions' and copies' integrity
- Emails that are extracted from their storage environment for use as evidence should be capable of being verified as having been stored in a compliant archival infrastructure

The Legal Detail Regards The Electronic Communications And Transactions Act

The Electronic Communications and Transactions Act is technology neutral so that it isn't dated as technologies evolve. This sets out certain features and technology neutral requirements for things like data storage and integrity. One important consequence of the Electronic Communications and Transactions Act is the fact that data messages such as emails, have about the same effect as a fax or letter in our law:

- Information is not without legal force and effect merely on the grounds that it is wholly or partly in the form of a data message.

Section 16(1) of the Electronic Communications and Transactions Act deals with retention, specifically, and states the following:

Retention.—(1) Where a law requires information to be retained, that requirement is met by retaining such information in the form of a data message, if:

a. the information contained in the data message is accessible so as to be usable for subsequent reference;
b. the data message is in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and
c. the origin and destination of that data message and the date and time it was sent or received can be determined.

One of the primary reasons for information to be retained is for evidentiary purposes. Sections 14 and 15 of the Electronic Communications and Transactions Act deal with originality and admissibility and evidential weight of data messages, respectively. In section 14, a data message is regarded as being an "original" if:

1. the integrity of the information from the time when it was first generated in its final form as a data message or otherwise has passed assessment in terms of subsection 14(2); and
2. that information is capable of being displayed or produced to the person to whom it is to be presented.

The manner in which integrity is assessed in terms of this Act is set out in subsection 14(2) which requires data integrity to be assessed:

1. by considering whether the information has remained complete and unaltered, except for the addition of any endorsement and any change which arises in the normal course of communication, storage and display;
2. in the light of the purpose for which the information was generated; and
3. having regard to all other relevant circumstances.

In the event it becomes necessary to introduce data messages into court proceedings, section 15 sets out a number of guidelines for assessing data messages' admissibility and evidential weight. The general rule is that the "rules of evidence must not be applied so as to deny the admissibility of a data message, in evidence:

1. on the mere grounds that it is constituted by a data message; or
2. if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form."

Section 15(3) goes further and requires that the information contained in data messages must also be given "due evidential weight". When assessing this "evidential weight", regard must be had to:

1. the reliability of the manner in which the data message was generated, stored or communicated;
2. the reliability of the manner in which the integrity of the data message was maintained;
3. the manner in which its originator was identified; and
4. any other relevant factor.

Section 15(3) suggests that changing the format of emails that are archived may comprise the emails' integrity because the process of changing the format may undermine both the "reliability of the manner in which the data message was generated, stored or communicated" as well as the "reliability of the manner in which the integrity of the data message was maintained". A conservative approach will be to preserve the emails in their original format although it is conceivable that conversion to archival formats like PDF may be found not to unduly prejudice these considerations.

Importantly and in a business context, section 15(4) introduced an expedited means of introducing this evidence in various fora and forms of proceedings in place of an more arduous mechanism in the Electronic Communications and Transactions Act's predecessor, the 1985 Computer Evidence Act:

A data message made by a person in the ordinary course of business, or a copy or printout of or an extract from such data message certified to be correct by an officer in the service of such person, is on its mere production in any civil, criminal, administrative or disciplinary proceedings under any law, the rules of a self-regulatory organisation or any other law or the common law, admissible in evidence against any person and rebuttable proof of the facts contained in such record, copy, printout or extract.

Section 17 is titled "Production of document or information" and states that a requirement that a person produce a document or information is met if that person produces an "electronic form" of the document or information as a data message and if:

1. considering all the relevant circumstances at the time that the data message was sent, the method of generating the electronic form of that document provided a reliable means of assuring the maintenance of the integrity of the information contained in that document; and
2. at the time the data message was sent, it was reasonable to expect that the information contained therein would be readily accessible so as to be usable for subsequent reference.

For the purposes of this particular section, integrity of the information produced is regarded as having been maintained if the information has "remained complete and unaltered" with the exception of any additional endorsements or immaterial changes which arise in the "normal course of communication, storage or display".