

Guide to Email Management

The information contained in this document has been prepared by the Forest Group and Michalsons Attorneys and is intended for general information purposes only. Do not make any business decisions on the basis of this information without consulting an appropriately qualified advisor who can analyse your precise requirements.

Link to records management

Email management is a category of “records management” which is concerned with the formal and systematic management of *business records* from “cradle to grave” – i.e. from birth to when they no longer serve a purpose and are disposed of. A *business record* is different from other types of information and documentation in that it has to be retained where a law says so, or should be retained when sent or received for business purposes.

In order for email records to be managed effectively they need to be linked to the functions, activities and decisions that they reflect. This is achieved by classifying or categorizing the e-mails according to a business classification scheme. This classification scheme forms the *solid foundation* upon which a variety of other e-mail related policies and procedures can be built and facilitates the implementation of e-mail retention rules and access.

Is it just data or is it a Record?

Email messages, including any attachments, created, collected, received or transmitted in the normal course of an organisation’s business which reflects the functions, business activities, and decisions of the organisation are **records and should be managed as such**.

An e-mail is a business record if a regulation or statute says it must be retained *; it contains valuable information about business operations; it contains info that must be filed with a regulator (e.g. the JSE or ICASA); it contains information used to negotiate a contract; a sales forecast depends on information it contains; it is the final version of a contract or it has business, compliance, historical, operational and/or legal value or significance to the organisation.

* Some of the more generally applicable laws are (i) requirements stemming from the right of access to information under PROATIA, (ii) general commercial requirements (e.g. Income Tax Act, Companies Act), (iii) general requirements regarding matters in litigation under Rules of Court, (iv) specific requirements for companies in the financial services sector (e.g. FAIS and FICA), (v) specific requirements for telecommunication companies and (v) specific requirements for government and government-owned entities (e.g. National Archives Act)

Examples of messages sent by e-mail that are business records include messages that initiate, authorize or complete a business transaction; messages received from external sources that form part of an organisational record; original messages of policies or directives; messages related to work schedules and assignments; agenda and minutes of meetings; briefing notes; final reports and recommendations.

Is there a Regulator of electronic records?

The National Archives is the Regulator of all electronic records created in the *public sector* in terms of their authority derived under the National Archives of South Africa Act 43 of 1996. The powers granted to the National Archives *do not* extend to the private sector. Therefore **there is no Regulator of electronic records in the private sector**.

This means that, *by and large it is up to individual organizations to determine how to retain and manage their electronic documents which includes email messages in a manner that promotes admissibility, evidentiary strength (weight) and satisfies legal and business requirements*.

Email records must be retained

ECT Act: There is a perception that Electronic Communications and Transactions Act 25 of 2002 (the ECT Act) makes record retention mandatory, including emails. This is not correct. The ECT Act does not make record retention mandatory; prescribe any minimum retention periods or introduce any criminal sanction for record retention non-compliance. There are several other statutes which impose an obligation to retain records. If the emails and their attachments qualify as business records, then they need to be retained according to the business, legal and / or historical value of the e-mail.

Sarbanes Oxley: The above perception is possibly borne out of a requirement under the Sarbanes Oxley Act (SOX), a law in the United States, which imposes criminal liability on any business that engages in document destruction, even if such document destruction occurs before the business has any formal notice of an official proceeding. SOX only applies to South African organisations who are listed in the US. The effect of SOX is that officers and directors of a company can be held criminally liable for the destruction of business records by its employees and representatives, even when such conduct is contrary to an official company policy.

King II: There is also a perception that King II makes it obligatory to retain records. This is not correct. King II is not a law. It is a Code and is designed to improve accountability and transparency of JSE listed public companies. King II states inter alia that “the board is responsible for the total process of risk management...” (3.1.1) and “should make use of...control models and frameworks...with respect to ... “safeguarding the company’s assets (including information)”. To *give effect* to the foregoing, organisations need to invest in the technology, people, and controls that will ensure that e-mail is retained and managed in a trustworthy fashion.

Bottom line: Email retention rules need to be developed and implemented so that e-mail records can be identified, retained, managed and disposed of in a systematic manner. This will enable an organisation to destroy all unnecessary e-mails in accordance with the provisions of its Record Retention and Destruction Policy and to demonstrate compliance with the legal retention requirements established by legislation. However, one must not lose sight of the fact that once records management obligations change when you are notified of an investigation, audit or legal proceedings. (Request our Record Retention and Destruction Policy brochure for further information).

Email records must remain intact for evidentiary purposes

Chapter 3 of the ECT Act permits the use of electronic documents, email messages, and other forms of electronic information as evidence. The golden thread here is the requirement to show an audit trail of “authenticity” and integrity of information. By “authenticity” we mean that it must be demonstrated that the evidence is what it purports to be. The authenticity of an electronic record (including email) can be challenged in many ways, including: by asserting that that it has been altered; by demonstrating that the system processes and procedures underlying the generation, communication, retention and retrieval of the record was not reliable; and by questioning the record’s authorship. In many cases, a successful challenge of an electronic record’s authenticity may not affect its admissibility as evidence, but rather will affect its persuasiveness or weight.

Where emails and their attachments are identified as records, they must retain their integrity in terms of their **structure** (layout or format and links to attachments and related documents), **content** (the information contained in the message) and **context** (information pertaining to the sender and recipients as well as any header information and transmittal data such as time and date).

The ECT Act does not, however, provide any guidance as to what the Courts will accept as constituting sufficient integrity. The need to demonstrate document integrity is also at the core of current best practices and standards which stipulate specific criteria for the management of electronic information, and they generally make clear that organizations are expected to manage electronic records and data in a manner that ensures its accuracy, completeness, reliability, accessibility, integrity, and trustworthiness. Ensuring integrity is not a product. It is a process that is made up of policy, process and technology (in the form of an appropriate records management system). Having a proper information management and record retention destruction policy (together with retention schedules) in place is key. So too is an information security policy as the email must be protected against unauthorized access, use, manipulation, destruction or loss.

Email should be captured into a records management system

E-mail messaging systems (such as Microsoft Outlook and Lotus Notes) were designed for transmission and receipt purposes only. They were not designed for ensuring the integrity and authenticity of e-mail records nor for implementing retention rules. As such e-mails identified as business records should be removed from messaging systems and stored in an appropriate records management system.

There are essentially 5 criteria that the Forest Group believes the system should meet:

- ✘ Is it capable of storing records in a trustworthy manner?
- ✘ Does the product protect the integrity, reliability, accessibility and accuracy of information throughout its lifespan?
- ✘ Does the product verify the accuracy of information during the recording process?
- ✘ Does the product provide long term content access?
- ✘ Does the product support records retention and disposition functionality?

Compliance with these criteria will also assist an organisation to ensure that the an email record satisfies the requirement of something having to be in "writing" (where it must be "accessible in a manner usable for subsequent reference" – per s12.b of the ECT Act), or that it be an "original" (if the email "is capable of being displayed or produced to the person to whom it is to be presented" – per s14.1.b of the ECT Act – and 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" – per s14.2.a of the ECT Act).

Adequate information security measures must be applied

In the absence of security features such as encryption, users of e-mail systems need to be aware that they cannot have assumptions or expectations of security or privacy with regards to their e-mails (where the emails can be likened to postcards instead of sealed envelopes). Should confidential, sensitive or attorney-client privileged content be distributed via email, then organisations need to implement robust security measures.

An effective email policy must be implemented

In addition to the need for the policies mentioned above, every organisation needs to establish a policy for capturing e-mail communications as records. Its own unique functions and environment should inform this policy. The policy should be endorsed by senior management and should be communicated throughout the organisation as part of the overall records management policy. The policy should inform e-mail users that official records communicated through e-mail systems must be identified, managed, protected, and retained for as long as is needed for ongoing operations, audits, legal proceedings, research, or any other anticipated purpose.

Staff must be trained

Clear roles and responsibilities for the appropriate use, management and disposal of e-mails need to be allocated to all organisational employees and functional departments.

E-mail policies are only effective when coupled to an employee training program. This training program needs to be comprehensive and ongoing and focused on instilling an employee sense of "ownership" with respect to the policy.

For further information please contact:

Johannesburg

Brad Abbott

Tel: (083) 661-1850
 Fax: (011) 507-5284
 E-mail: brad@forestgroup.info
 Web site: www.forestgroup.info

Cape Town

Lance Michalson

(021) 438-6323
 (011) 507-5284
lance@forestgroup.info
www.forestgroup.info