Implementing a Policy for ELECTRONIC CONTENT AND SYSTEMS MANAGEMENT

Editor's Note: This article is excerpted from the new technical report *Implementing Electronic Messaging Policies* (ARMA International 31-2018), which is available at *www.arma.org/store/ViewProduct.aspx?ID=11017155.*

Managing electronic messages identified as records includes assigning responsibility for managing message content and systems. To this end, the organization may limit the locations in which electronic messages can be maintained, particularly those locations outside the organization's direct control, such as an employee's home computer or mobile device, portable storage media, or third-party servers. The electronic messaging policy addresses the following:

- Appropriateness of content
- Attachments
- Drafts
- Duplicates
- Threads
- Metadata
- Monitoring

Appropriateness of Content

The electronic messaging policy encompasses guidance related to the types of messages and appropriate content allowed by the organization. The policy specifically addresses those items by:

- Emphasizing that electronic communications are to be accurate, with users exercising the same care in writing them as they would for any other written communication to a formal audience

- Identifying messages, files, and information not to be sent by unencrypted electronic communications, such as:
  - Attorney-client privileged information
  - Confidential and personal information, such as salary or medical records
  - Copyrighted, proprietary, secret, or other organization-confidential information
- Providing users with a standardized header/footer statement to declare intent and protect the user and the recipient from liability when technological or human error allows the message transmission to unintended parties
- Providing users with a style guide that presents specific examples of recommended electronic message style and usage
- Specifying whether personal, non-business use of the messaging system is prohibited; if permitted, within what circumstances and limits
- Stating whether the organization has the right, at its discretion, to monitor electronic message system content; if applicable, identifying the conditions under which monitoring can occur
- Warning that content that is misleading, inaccurate, fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, or in violation of laws or regulations is prohibited

Attachments

Attachments or linked items – such as audio, photo, text, or video files, embedded objects, images, or hyperlinks – can be associated with any electronic message identified as a record. To open an attachment or linked item, the end user may need a specific application, separate from the electronic messaging application.

Metadata, which is structured information that describes both paper and electronic information, is particularly important when associated with electronic messages identified as records; it provides the information by which those records are located and managed.

Generally, policies and procedures for appraising and scheduling attachments or linked items are identical to those of their non-electronic counterparts. The electronic messaging policy should be clear about the mode of retention of attachments or linked items to ensure consistency and avoid duplication; this can be especially important when multiple or separate recordkeeping systems are used for storing electronic messages or linked attachments. Also, the policy will stipulate that as with other electronic records, naming conventions and version control procedures are instituted to ensure easy identification of current versions.

Drafts

Usually, electronic message drafts are not retained. The electronic messaging policy specifies circumstances under which drafts are retained. Each organization's policy, in accord with other records-related policies, specifies circumstances under which drafts are records and, as such, are subject to management during the information life cycle.

Duplicates

Organizations commonly use electronic messaging systems to disseminate information to multiple recipients. Depending on the types of electronic messaging systems in use, this practice could result in the creation of multiple copies of the same message. Each organization's electronic messaging policy, in accordance with other records-related policies, specifies which copy is to be considered the record and, as such, is subject to management during the information life cycle.

Threads

A thread, also called a string, is an electronic messaging conversation comprising multiple messages. The conversation can be broken or continuous over time. The electronic messaging policy specifies how the content of threads is identified, how threads with diverse or changing content are classified, and how threads are filed.

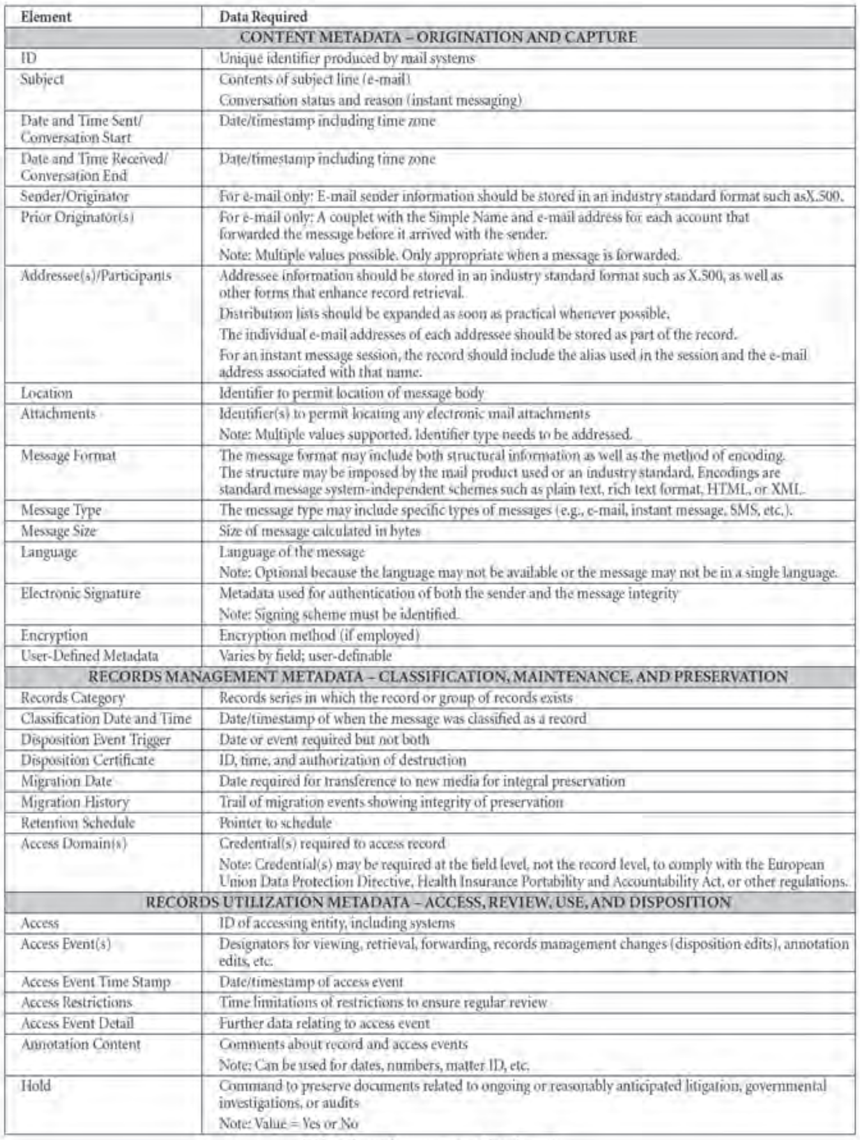
Metadata

Metadata, which is structured information that describes both paper and electronic information, is particularly important when associated with electronic messages identified as records; it provides the information by which those records are located and managed. In addition, metadata:

- Serves as the mechanism for documenting the life cycle of information, including creation, usage, and disposition
- Identifies relationships between information items and preserves the context of a particular piece of information
- Documents how that object behaves (i.e., its function, use, and relationships to other information objects)

Metadata is used to ensure the authenticity, reliability, integrity, and usability of the record.

Because authenticity, reliability, and integrity describe trustworthy documents from the legal perspective, metadata can be used to identify a record as a legally accept-



Element	Data Required
CONTENT METADATA – ORIGINATION AND CAPTURE	
ID	Unique identifier produced by mail systems
Subject	Contents of subject line (e-mail) Conversation status and reason (instant messaging)
Date and Time Sent/ Conversation Start	Date/timestamp including time zone
Date and Time Received/ Conversation End	Date/timestamp including time zone
Sender/Originator	For e-mail only: E-mail sender information should be stored in an industry standard format such asX.500.
Prior Originator(s)	For e-mail only: A couplet with the Simple Name and e-mail address for each account that forwarded the message before it arrived with the sender. Note: Multiple values possible. Only appropriate when a message is forwarded.
Addressee(s)/Participants	Addressee information should be stored in an industry standard format such as X.500, as well as other forms that enhance record retrieval. Distribution lists should be expanded as soon as practical whenever possible. The individual e-mail addresses of each addressee should be stored as part of the record. For an instant message session, the record should include the alias used in the session and the e-mail address associated with that name.
Location	Identifier to permit location of message body
Attachments	Identifier(s) to permit locating any electronic mail attachments Note: Multiple values supported. Identifier type needs to be addressed.
Message Format	The message format may include both structural information as well as the method of encoding. The structure may be imposed by the mail product used or an industry standard. Encodings are standard message system-independent schemes such as plain text, rich text format, HTML, or XML.
Message Type	The message type may include specific types of messages (e.g., e-mail, instant message, SMS, etc.).
Message Size	Size of message calculated in bytes
Language	Language of the message Note: Optional because the language may not be available or the message may not be in a single language.
Electronic Signature	Metadata used for authentication of both the sender and the message integrity Note: Signing scheme must be identified.
Encryption	Encryption method (if employed)
User-Defined Metadata	Varies by field; user-definable
RECORDS MANAGEMENT METADATA – CLASSIFICATION, MAINTENANCE, AND PRESERVATION	
Records Category	Records series in which the record or group of records exists
Classification Date and Time	Date/timestamp of when the message was classified as a record
Disposition Event Trigger	Date or event required but not both
Disposition Certificate	ID, time, and authorization of destruction
Migration Date	Date required for transference to new media for integral preservation
Migration History	Trail of migration events showing integrity of preservation
Retention Schedule	Pointer to schedule
Access Domain(s)	Credential(s) required to access record Note: Credential(s) may be required at the field level, not the record level, to comply with the European Union Data Protection Directive, Health Insurance Portability and Accountability Act, or other regulations.
RECORDS UTILIZATION METADATA – ACCESS, REVIEW, USE, AND DISPOSITION	
Access	ID of accessing entity, including systems
Access Event(s)	Designators for viewing, retrieval, forwarding, records management changes (disposition edits), annotation edits, etc.
Access Event Time Stamp	Date/timestamp of access event
Access Restrictions	Time limitations of restrictions to ensure regular review
Access Event Detail	Further data relating to access event
Annotation Content	Comments about record and access events Note: Can be used for dates, numbers, matter ID, etc.
Hold	Command to preserve documents related to ongoing or reasonably anticipated litigation, governmental investigations, or audits Note: Value = Yes or No

Table 1: Electronic messaging metadata elements

able document when presented as evidence in a legal proceeding. In addition, metadata maintains the context of a record and supports searching, retrieval, and display.

The management of metadata should be handled by IM professionals and linked with the records retention policy. This includes:

- Establishing security and privacy policies that define which metadata should be retained and for how long
- Mandating which metadata is editable and which is not
- Specifying which metadata becomes part of an audit trail
- Stating which metadata can be accessed by which entity

For preservation purposes, metadata is essential to retaining records in a useful state over time. These metadata elements are used to define object characteristics, such as size, format, creating application, signature information, and fixity. Metadata can be stored with the record (e.g., e-mail messages with descriptive headers) or stored separately (e.g., in an external catalog).

An advantage of storing metadata with the record is that when the record is copied or moved, the metadata moves with it. When the record is deleted, the metadata is deleted, as well. A disadvantage of having only embedded metadata is that all records need to be examined to satisfy a query.

The advantage of storing metadata separately is that it can make searching more efficient, since fewer servers need to be accessed to locate the record. However, with this method, automatic linkages can be lost, and additional steps are needed to ensure that a record is not copied, moved, or deleted without modifying the associated metadata.

Electronic messages may provide embedded information (metadata) generally not found in other electronic records that may be useful to information professionals, including a description of the originating system, the method of transport, and the intermediate agents.

Metadata for records in the form of electronic messages fits into three broad categories: content metadata, records management metadata, and records utilization metadata. These categories, included in Table 1, describe metadata captured or added as a result of life cycle activities. Table 1, while not all-inclusive, offers a preliminary list of metadata elements relative to electronic messaging.

Monitoring

The organization oversees the use of its systems to ensure compliance with policies and to determine that systems are not being used for illegal or other improper purposes. The electronic messaging policy addresses the monitoring of electronic messages and systems as organizational resources. The policy states:

- The circumstances under which the monitoring occurs
- The penalties resulting from improper use discovered by such monitoring
- The scope or extent of the monitoring

For more on this topic as it relates to monitoring for internal audit or legal compliance, see section 5.4 [of the technical report from which this article was excerpted]. E