

# **Policy on Electronic E-Mail as Records**

## **Draft – Last Revised June 27, 2001**

### **PURPOSE**

The purpose of this policy is to establish an e-mail policy for all University departments and offices that create, use, and manage e-mail as part of the daily transaction of business.

### **SCOPE**

This policy applies to all e-mail and e-mail attachments created or received by University personnel within the entire Indiana University system.

### **STATEMENT OF AUTHORITY**

Authority for this policy is derived from the University groups responsible for the effective management of IU's information resources: the Committee on Institutional Data, the Committee of Data Stewards and the Indiana University Archives. This Committee on Institutional Data is comprised of vice presidents, deans and directors and is charged with establishing overall policy and guidelines for management and access to the institutional data resources of Indiana University. The Committee of Data Stewards is comprised of university and campus officials who have planning, policy and operational responsibilities for the management and use of institutional data. The Data Stewards, as a group, are responsible for recommending policies and establishing procedures and guidelines for university-wide management of institutional data. The University Archives, a division of the Indiana University Libraries, is authorized to establish and promulgate standards, procedures and techniques for the effective management of University records. It is also responsible for preserving the University's documents and records of historical value.

### **BACKGROUND**

The effective management of e-mail is one of the primary objectives of IU's records management program. E-mail messages may qualify as business records, and in some cases, may be the only record created that documents a transaction, an action taken, or a policy determination or interpretation. It is therefore extremely important that all University personnel recognize the significance of the e-mail messages they create or receive and manage them properly.

### **RELATED POLICIES:**

See also the *Electronic Records Policy* for requirements for the responsible management of electronic records and information systems.

## **POLICY SUMMARY**

The following elements shall be present in an electronic recordkeeping system to ensure the reliability, accuracy, security, and accessibility of the e-mail it manages:

- models of business processes that assist in the identification, capture, maintenance, and scheduling of e-mail that is a business record.
- filing systems that assist in the easy storage, retrieval and destruction of e-mail.
- policies and procedures that monitor the security and access and ensure the authenticity and reliability of e-mail and the reliability, integrity, and security of the system hardware and software.

## **IDENTIFYING RECORDS**

### **Record Status**

- E-mail that is received or created in the course of undertaking and completing a business transaction is a record.

### **Definition of a Record**

- Recorded information, in any form, created or received and maintained by an organization or person in the transaction of business or the conduct of affairs and kept as evidence of such activity.
- Evidence of a business transaction, with evidence defined as documentation on the content and structure of the records and the context of its creation.

### **Business Process Modeling**

- Departments shall develop models of business processes to determine where and when e-mail messages are created and used in the course of completing business transactions.

## **FILING AND MAINTAINING RECORDS**

### **Capture**

- E-mail that fits the definition of a business record shall be captured in an electronic recordkeeping system and maintained as a business record with all relevant content, context, and structure metadata.
- If the preferred method of capturing e-mail records within an electronic recordkeeping system cannot be met, then:
  - E-mail, with appropriate contextual detail, can be printed and filed into a paper-based recordkeeping system, or
  - Recordkeeping functionality can be built into the electronic messaging system.
- Back up tapes are not considered a form of a recordkeeping system, and therefore, are not an acceptable format for capturing and maintaining e-mail records.

**Filing**

- E-mail of similar or like transactions shall be organized into a coherent filing system that will facilitate access, retention and disposition.

**Metadata**

- E-mail shall be captured and maintained with essential metadata describing the content, context, and structure of the message.

**Attachments**

- Attachments to e-mail shall be preserved for as long as the e-mail message itself is maintained.

**Distribution Lists and Aliases**

- Captured e-mail shall maintain the actual e-mail addresses for all senders and recipients.

**Encryption**

- Encryption is acceptable for transmission of e-mail, but messages shall be stored in an unencrypted form.

**Access and Use**

- E-mail shall remain accessible and usable for as long as it is required to be retained to meet all administrative, legal, fiscal and historical requirements.
- Access to e-mail records shall be restricted to authorized users.

**System Security**

- Security and access policies shall be developed to protect the e-mail records from alteration or unauthorized use.

**Scheduling and Disposition**

- Like other business records, e-mail shall be retained or disposed of in accordance with authorized and approved records retention schedules.
- Retention of all e-mail records maintained in electronic files is the same as for similar records maintained in traditional paper formats unless otherwise specified.

**Preservation**

- The future usability of e-mail shall be ensured through the development of conversion strategies designed to update hardware, software, and storage media.

## **MANAGEMENT OF RECORDS**

### **System and Procedural Documentation**

- Policies, guidelines, and procedures defining systems requirements and all implementation activities related to e-mail records shall be created and distributed to all personnel.

### **Responsibility**

- The Committee on Institutional Data and the Committee of Data Stewards shall be responsible for the development and maintenance of the e-mail records policy.

### **Sanctions**

- Failure to comply with any of the above guidelines is in violation of University policy and disciplinary action may be applied.

### **Review**

- A periodic and cyclic (every 3-5 years) review of this policy shall be undertaken to keep the e-mail records policy current with best practices and new technology.

### **Definitions that need to be attached to the policy:**

- E-mail system
- Business process modeling
- Metadata
- Recordkeeping system
- Retention and disposition schedules
- Encryption
- Migration
- Back-up tapes