

**Domestic and Foreign Missionary Society
Records Retention and Management Policy Proposal**

Records Retention and Management Policy

I. Purpose	1
II. Policy Statement	1
III. Scope of Coverage	1
Records of the Society and the General Convention.....	1
Business Records and Processes	2
IV. Records Management	2
V. Responsibility and Accountability	3
VI. Administration	3
Enterprise-wide Records Management.....	3
Email and Electronic Communications	4
Legal Discovery and Hold.....	4
Security.....	4
Access to Non-current Corporate Records	5
Destruction of Records.....	5
Additional Considerations Regarding Electronic Records.....	5



Records Retention and Management Policy

I. Purpose

This policy addresses the need of the Domestic and Foreign Missionary Society (the Society) and the General Convention to follow standard policies and practices for the retention, disposition and systematic management of organizational records. The reasons for having a records management policy include: securing access to records that are essential to ongoing operations, ensuring business continuity in the event of unanticipated events, reducing exposure to unnecessary fiscal and legal liabilities, responding effectively to discovery requests, reducing costs of information management, and preserving information assets and institutional memory. In the current record keeping environment, a records management policy includes these goals:

1. A common understanding of the definition and scope of the Society's records
2. Controls over retention and disposition of records in compliance with regulatory requirements and administrative standards
3. Provision for the management of electronic records and communications
4. Ongoing maintenance, audit and storage of records
5. Definition of responsibilities of the record creator and other records custodians

II. Policy Statement

This policy, together with approved procedures and management standards, establishes requirements for the retention, disposition, maintenance, and preservation of the Society's records in all formats and media, including electronic records and communication, in accordance with statutory and regulatory standards, and appropriate administrative standards and best practices. All business records will be scheduled and maintained for a minimum required retention period, and thereafter as necessary for archival purposes. No record will be improperly or prematurely disposed of by any employee. All Society employees are obligated to follow the Society's records retention and management procedures as established by this policy.

III. Scope of Coverage

Records of the Society and the General Convention

This policy affirms that a record of the Society and the General Convention is information that is recorded or captured as evidence of the organization's business activities and transactions. **The Society's records are the records created or received by any officer or agent of the Society in the exercise of their fiduciary responsibility.** This policy covers information that is in a fixed form and recorded on standard media and formats, including documents on paper (e.g., reports, minutes, blueprints), printed publications (e.g., DFMS and General Convention publications), electronically stored information (e.g., databases, text documents, digital images), electronic communication (e.g., emails and list postings), electronic records, and electronic publications (e.g., websites, intranets).

A full definition of what constitutes a record for purposes of records retention and management of the Society's records is found in Canon I.5.2:

Records are defined as all fixed evidential information regardless of method, media, format or characteristics of the recording process, which have been created, received or gathered by the Church, its officers, agents or employees in pursuance of the legal, business and administrative function and the programmatic mission of the Church. Records include all original materials used to capture information, notwithstanding the place or conditions of creation, or the formality or informality of the characteristics of the record. The records and archives of the Church are not limited by the medium in which they are kept and include such formats as paper records, electronic records, printed records and publications, photo-reproduced images, and machine-readable tapes, film and disks.

Employees of the Society are required at the time of hire to acknowledge the Society's ownership of records as work product and works-for-hire by signing the statement, "Ownership of Records, Files, Documents and Other Papers Produced by Employees of the Society During the Course of Employment."

Personal records are not records of the Society, and this policy does not cover records produced by employees in the course of activities unrelated to their employment or the work of the Society. Personal records should not be kept in the Society's paper files or electronic record keeping and information storage systems.

Business Records and Processes

The scope of the business records produced by the Society and the General Convention includes corporate responsibilities, canonical mandates, and mission programs. Retention and disposition of the Society's records include all records created by employees while performing the work of the Society.

The business processes of the Society include the exercise of executive and primatial leadership, administration of corporate functions in human and material resources, management of finances and investments, use of information and communication technologies, support of the General Convention and its official bodies, implementation of the General Convention's mission program, development of ministry, and maintenance of jurisdictional affiliations. (An outline of the Society's business processes is maintained by the Archives and can be found in a discussion document attached to this statement.)

IV. Records Management

The fundamental principles of records, information, and archival management are applicable to both paper and electronic records. These principles include appropriate organization, maintenance, and disposition of the records.

- **Organization of Records.** Records should be organized and kept in identifiable filing scheme structures throughout the life cycle of the record from office use to inactive custody in the Records Center or Archives. Once a record is declared by the creator, the record should be filed or stored in the filing system. The Archives and Records Management staff will work with the individual and department to identify useful and logical filing schemes.
- **Maintenance, Security and Authenticity.** Keeping authentic records after the point of current business use requires that they be set apart with all the features of their initial creation and use. The Archives will retain records as approved and scheduled in a secure environment and provide controls to ensure that paper records are kept in their original form. The Archives will work with the information technology personnel (e.g., MIS and Communications offices) to create retention and accountability controls over electronic records. The most effective way to guarantee authenticity for electronic records is to implement enterprise-wide electronic records management.
- **Retention and Disposition of Obsolete and Legacy Records.** Paper and electronic records will be retained for ongoing business use, and ultimately destroyed, retired, or refreshed for future use. These activities are conducted in accordance with the Society's records retention schedule and management policies. The appropriate destruction of paper and electronic records, including confidential business and personal data, will be supervised by the Archives' records management officer and documented for audit purposes using standard destruction logs and records schedules.

V. Responsibility and Accountability

Responsibility for managing the records of the DFMS and the General Convention is shared between the individual record creator, the departmental custodian of the record, and the keeper of the Society's records (the Archives). Other officers and agents have an important role in securing the Society's records. These centers of accountability are:

- **Executive management (COO and senior management).** Reviews and approves retention recommendations, enforces policy compliance, and secures resources for records management
- **Records management staff (Archives).** Implements policies and procedures for the retention and disposition of records in all formats, and carries out records management for offices and agencies of the DFMS and the General Convention.
- **Information management and communications systems staff (MIS and Communications).** Act as managers of networked information, electronic mail and communication, Website publications, and electronic documents in content management systems. These departments work with Archives to secure electronic records as designated for temporary or permanent retention.
- **Departmental managers and staff.** Each employee and manager is responsible for retaining and identifying records as prescribed in all formats, reviewing and acknowledging retention policies regarding specific records, and working with Archives to comply with the Society's policies on records retention and the orderly retirement of records that fall within the scope of their work.

VI. Administration

Enterprise-wide Records Management

This policy represents a change from the existing situation of ad hoc retention guidance and compliance to uniform standards applied across all offices of the Society for all record formats. The following operations form the basis for the Society's records management program.

- Electronic records and communication are integrated with the management of other records and information resources of the Society's workplaces. The implementation of an enterprise-wide model of records management is facilitated by using an electronic document and records management system (EDRMS) to integrate the management of all record formats.
- Each department will identify an individual who acts as records liaison to the Archives' Records Management Office to assist in implementing retention and management policies for unit and departmental records, including both paper and electronic records.
- Department managers will consult with the Archives' staff to examine any policy-related implications of new record keeping systems in order to address retention, content management, and access-related issues before adoption. **This is a critical design step** before deploying new electronic information systems or major enhancements to existing systems.
- The Archives will maintain an auditable inventory of the Society's electronic records and information systems, specifying the location, manner, and media in which electronic records are maintained to meet operational and long-term archival requirements.

- The MIS office will work with the Archives to identify and verify the existence of, and develop and maintain up-to-date documentation about, all electronically stored information and electronic record keeping systems that hold current data applications and legacy files.
- The Archives develops and implements approved records retention and disposition schedules for the Society's records. Records retention schedules include electronic records wherever they are created by the Society's employees, offices or agents.
- Department managers are to work with the Archives and MIS to establish procedures and safeguards to ensure that the requirements of this policy are applied to electronic records that are created or maintained by third parties contractors or as remote web applications.
- Archives will provide training to users of software and electronic mail systems on record keeping requirements, procedures for designating email as records, and moving or copying records for inclusion in a record keeping system.

Email and Electronic Communications

Email created in a work-related capacity utilizing the information systems of the DFMS are records of the Society. Each employee acknowledges and observes the Society's rules for using its email system upon hiring (e.g., "Proper Use of DFMS Computer Resources", dated May 14, 2004). Individual employees are responsible for managing email messages and attachments for purposes of declaring a retained record or destroying messages that are considered transitory or obsolete for purposes of transacting the business of the Society. Email messages are scheduled for retention or destruction. Messages deleted by the records creator as transitory or obsolete will be scheduled for destruction. Records retained by the record creator will be retained according to a schedule and reviewed for archival retention.

Legal Discovery and Hold

The Society has been and may in the future be served with a subpoena or a legally mandated request for records. Employees may become aware of or suspect a potential legal action, a civil investigation, an audit, or other legal demands and discovery requests concerning the Society's business activities and programs. In such circumstances and events, employees shall suspend all document destruction, disposal, and deleting activities as necessary to comply with laws. Employees should seek the advice of the Society's counsel. Counsel shall immediately inform the Archives' staff of the hold. Archives' staff will take all appropriate and necessary steps to secure all documentation from further disposition, and shall assist in informing all other appropriate staff of the suspension of records destruction, including but not limited to those responsible for electronic information storage and records keeping systems.

Security

The security of records held in the Record Center is the responsibility of the Archivist for Records and Information Management Services. Except in urgent circumstances, physical access to the Records Center takes place under the supervision of the records management officer or other Archives' staff. Access to the contents of the Records Center is managed through inventory records kept by the Archives. Security for electronic records maintained as active or legacy records in the ECC's networked information systems is the responsibility of the enterprise technology services office (MIS). Security for electronic records maintained as active or legacy records in Field Offices of the Episcopal Church Center is the joint responsibility of the Field Office, the host technology services office, the MIS office, and the Archives. Access to electronically stored information for purposes of establishing retention and

inventory control of the Society's records is managed through the enterprise-wide electronic document management system and is the joint responsibility of the Archives and the creating office or departmental management.

Access to Non-current Corporate Records

Employees are responsible for controlling access to active records. Records transferred to Archives are accessible to the record creator and their successor agents. External access to unpublished corporate records that are less than 30 years old is restricted. Access to restricted records is granted through the department head, the chief executive officer, or the Canonical Archivist or the delegate thereof in a matter of legal or corporate importance. Access to personnel records, records of a private or personal nature, and other records identified by the creator and the Archives as confidential file series are restricted for a period of 80 years. The Board of the Archives and the Executive Council establish access policies for the Episcopal Church's inactive records and archives.

Destruction of Records

Decisions on what should be destroyed and when should be based on the content of records without consideration to their format. Inactive records with no operational, legal, fiscal or historical value are destroyed according to approved records retention schedules. In the event that a record is new, or has not previously been scheduled, it is analyzed for its business purpose and scheduled for destruction. An Archives staff person supervises the certified physical disposal of scheduled records and maintains standard destruction registers. The Archives will use electronic records management software to ensure an independently verifiable audit trail exists for the scheduled destruction of electronic records, including proper disposal of back-up copies.

Additional Considerations Regarding Electronic Records

Federal Rules of Civil Procedure make electronic record discovery the norm and raise the expectation that every organization will be able to identify an inventory of information sources and be able to generate information outputs. The Archives is responsible for the regular survey of the Society's electronically stored information, and for identifying all structured and unstructured electronic records. The survey will include the physical and logical location of network servers containing any and all electronic records of the Society, including records held by third-party vendors.

The Archives will prepare and apply records retention schedules for the Society's electronically stored information and records, including the Society's Web content, Internet publications, electronic messaging, voice mail, peer-to-peer collaboration, intranets, PDAs, Web 2.0 communications, and all other electronically stored information formats yet to be devised. Practices will be developed to permit disposal or retention of discrete data sets in accordance with legal, administrative, or historical requirements. Archives' staff will analyze and recommend electronic storage requirements for the Society's permanent and long-term retention of electronic records.

Electronic records depend on systems that enable a person to review, evaluate, and transfer non current and legacy records to a read-only archive server. Transactional computer records will be kept and maintained to create an audit trail of all system and data application processes, and all user activity. Archives and MIS will work together to identify the best technological solutions for the long-term retention and preservation of electronic records, while meeting wherever possible the goal of General Convention Resolution 2006-A049 (Adopt Open Standards for Data). The Society will find the resources to be in compliance with General Convention and other regulatory requirements that affect electronic records.

Employees' electronic records will normally be created, maintained, and/or backed-up on the Society's networked computer systems. This policy covers all of the Society's records, including electronically stored information maintained on host data servers in the Society's field office or remotely by third-party contractors. Routine practice and contingency plans for data back-up systems and disaster recovery for vital records will be documented and regularly updated. The MIS office, and any departmentally contracted IT staff working independently of the Society's MIS office, are responsible for notifying Archives staff at the earliest opportunity of any plans to update, retire and/or migrate active or legacy files to new applications or storage environments. No one should destroy electronic data sets or legacy records without notifying and getting permission from the Archives first. The Archives will evaluate the electronic records on the basis of existing laws and regulations, professional standards, best practices, and evidential value, and then assign a retention period.

Degrees of security required for file storage and management will reflect the sensitivity and confidential nature of any recorded material. Authorized Archives staff will have read-only clearance for purposes of implementing retention, disposition, indexing, and maintenance of all non-current and legacy electronic records stored in the Society's computer systems. Appropriate security systems, notification procedures, and restrictions will be established to protect privacy and confidentiality. As appropriate and within policy, legacy electronic records will eventually be made accessible for Church-wide research.

Implementation of these requirements and best practices is assured by deploying technological solutions that match the technology being managed. While some piecemeal measures can be taken to identify retained electronic records and dispose of obsolete electronic records, the Society is best served by deploying an electronic document and records management system (EDRMS) for an enterprise-level management solution to electronic records retention and disposition. An Implementation Discussion accompanying this policy statement contains an elaboration of the features and advantages of an EDRMS.

Rev. 04-17-2009