**Domestic and Foreign Missionary Society**
**Records Retention and Management Policy**
*Approved by Executive Council, April 22, 2009*

**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*

**The Archives of the Episcopal Church**
**Policy for the Selection of Software for Records of The Episcopal Church**

The following questions will be used by DFMS departments and staff who are considering a new electronic record keeping or data management system. New systems can be in-house DFMS computers, or a service provider working with cloud computing systems outside of the DFMS network. Long term access to electronic records is costly if retention is not built into the data design and structure of a record keeping system at the beginning. The questions found in this policy will be used as a checklist to evaluate a vendor or product offering. The Archives' Records Management Office will work with staff to answer these questions in order to ensure compliance with the DFMS Records Retention Policy and best practices for the security of electronic records of the DFMS and the General Convention (the Church).

> *Special Note: Staff of the Archives/Records Management and MIS office will assist DFMS employees in planning and implementing new computer software systems, and will provide guidance on how and when to apply these policies to protect the records of the Society.*

## When to Apply This Policy and Its Guidelines

DFMS staff will consult with the Archives and appropriate information technology staff in the following circumstances:

- Purchasing or developing a new software system
- Preparing an RFP or consulting with an outside IT vendor or contractor
- Replacing an old software system containing legacy data
- Implementing a major upgrade of a software system already in place
- Any instance of software use and data storage with "cloud" service providers (e.g., GoogleDocs, Basecamp, UltiPro) that use non-DFMS servers to create or store records
- Beginning major new projects that will require document tracking and management

## When the Policy Guidelines May Not be Useful

These policy guidelines are ***not*** meant to be used for creating common office documents (correspondence, PowerPoint presentations, meeting minutes, etc.) kept on the DFMS network using our standard suite of computer software (Microsoft Office). It is unnecessary to use these policy guidelines to evaluate existing DFMS software (e.g., Word, Excel) used for existing and routine work processes. Remember to consult the Archives about new records, however, so that they can be covered by the DFMS Retention Schedules, which in the future will be used to retire data automatically.

## Policy Guidelines

### 1.0 General Considerations on Data Custody, Migration and Delivery

1.1 Is the application open source or proprietary? What is the format of the data?

1.2 Does the contract explicitly state that the *data* remains wholly the property of the DFMS regardless of where it is physically stored? If this is a custom-made application, will the *application* belong wholly to the DFMS, including program, code, maintenance and operational manuals?

1.3 Will legacy (i.e. inactive but valuable) data be transferred to the new application? If not, what is the status of the old data; where is it and is the system still operable?

1.4 Has the DFMS Department retained paper records associated with the development and design specifications of the system (e.g., system input and output documents, workflow documents, functional requirements)?

1.5 Is the system capable of creating a periodic report for long term retention, i.e., a "snapshot" of data at regular intervals? What kind of data capture would truly represent the record? A quarterly or annual snapshot? A particular kind of report? Have you consulted with the Archives about this record?

1.6 Does the system produce standard output for document sharing and retention, including XML, PDF, XSL? Others?

1.7 Is the information contained in the system valuable and understandable when output as a flat data file (.txt), i.e., without the functionality of the application?

1.8 What hardware and operating systems are in use? Are these compatible with the Department's and the DFMS's systems?

1.9 With regard to software and/or hardware upgrades, does the service provider guarantee that the customer will be notified prior to either an upgrade or any data migration that might occur?

1.10 Will the system use electronic signatures? If so, do the signatures meet state and federal requirements for electronic signatures?

1.11 Does the application maintain an accessible transactional log and audit trail by which you can track changes and access to the records?

1.12 How will the system draw together all metadata elements to create a metadata profile for each record?

1.13 Does the system persistently link or embed the metadata profile to the record?

1.14 Does the system keep a unique identifier with the record as long as it exists?

## 2.0 Service Provider Reliability

2.1 What is the ownership structure of the provider (corporation, sole proprietorship, other)?

2.2 How many years has the service provider been in business?

2.3 Where is the business located and where the data storage devices located physically? Who owns the property that houses the data storage devices?

2.4 Has the DFMS conducted a due diligence background check on the contractor's functional and legal status?

2.5 Have you submitted all business agreements for legal review?

2.6 What guarantees are offered by the vendor/contractor as service provider such that a bankruptcy or business failure does not result in a shut down of the data center or an unplanned removal of data storage and access?

2.7 Is a third party trustee named in the service provider's standard contract, insurance certificate, or audit statements?

2.8 What subcontracted services does the provider use? Who are the subcontractors and where are they physically located?

2.9 If using a software service, is the software source code held in escrow and through what entity would it be accessed?

2.10 Have you obtained a certificate of the service provider's insurance and established that adequate coverage exists, including the name of a third party trustee, in the event of an incident of data corruption, data theft, or other loss?

## 3.0 Access Control and Document Management

3.1 Who will have access to the data at the service provider's operation? What access restrictions have been enabled for high risk personal data?

3.2 Have access provisions been identified and put in place for DFMS's MIS and Archives-Records Management to exercise backup security controls on behalf of the user? What global mechanisms are in place to "lock down" the data as records so they cannot be altered but can still be read?

3.3 Are document-level controls in place to allow certain users to create and revise documents, while allowing "read only" rights to others?

3.4 What indexing tools are supported, and can the customer's in-house indexing terms be accommodated?

3.5 What audit provisions exist to record access to the data set (read and write)?

3.6 What are the available bandwidth and data transmission speed?

## 4.0 Electronic Records Discovery

4.1 What are the service provider's recommendations and methodologies for marking and segregating records identified as being under a legal hold?

4.2 For records subject to government regulations, for example employment records or financial records, will the vendor guarantee the delivery of the data in the format required by law in case of an audit or legal inquiry? As the DFMS staff person, have you thought about what documentation you will need?

4.3 How are multiple access restrictions implemented so that a legal request to limit access to certain records identified as restricted under a legal hold does not affect access to other records not covered by a hold?

4.4 What evidence does the service provider give to demonstrate that the Church's records are kept separate, and not mixed with another corporation's data?

4.5 What provisions exist to ensure that records covered by a legal hold cannot be deleted or altered until an authorized release is made on the hold?

4.6 Describe the protocols or processes in place by which the service provider segregates and secures records placed on legal hold on both the primary and backup servers, and other storage devices.

## 5.0 Retention and Disposition of Non-current and Legacy Electronic Records

5.1 Have you asked for the system to retain a history file of changes to the records or will the data be permanently overwritten with each revision?

5.2 Have you checked with Records Management/Archives staff to identify and include an appropriate retention period for the information stored in any <u>new</u> record keeping system of the DFMS? Is the recorded information represented on the DFMS corporate Records Retention Schedule?

5.3 How will the system manage changes in records management requirements resulting from new business needs or regulatory requirements? Will the system support changes to a retention determination?

5.4 Has the DFMS department worked with the Church's designated official to identify the disposition status for legacy (inactive but still valuable) data according to DFMS retention schedules?

5.5 What are the procedures in the system for the user to carry out DFMS or General Convention records retention requirements for new applications or for legacy records created in the process of introducing a new system?

5.6 Will the system internally support an automatic, scheduled retention request for any record or set of records? What are the redundancies and deletion routines for retained data? Are the records sequestered or simply tagged?

5.7 How will the system's records retention performance be tested and measured?

5.8 During software upgrades, what provisions exist for retention and audit of legacy records?

5.9 Have the protocols been put in place by the DFMS department for the way in which the legacy or historical data will actually be transferred to the Archives? (See also section 1.6 on acceptable formats.)

5.10 Are destruction certificates produced to cover all storage and backup systems to ensure that a total purge of all specified records, including recovery devices, has occurred at the Church's request?

## 6.0 Return of Data

6.1 At termination of contract, how will the service provider migrate data to a new service provider or to the DFMS department and/or the Archives? Is the migration format specific?

6.2 What measures or tracking devices does the DFMS office use (i.e., a checklist, an inventory, or other audit control) for identifying data that should be migrated at the end of a vendor contract?

6.3 What data formats are available in the event of a request for return of data, and what role does data compression play in returning data in its original format?

6.4 How is data return enforced with subcontractors, especially vendors in other countries covered by different laws and regulations?

6.5 Does the service provider use compression or encryption software or hardware that could create migration concerns?

6.6 Is there any proprietary software in use that could make the data obsolete if the software is no longer supported? If proprietary, does the software utilize open content data interoperability (Content Management Interoperability Services standard) for data capture?

## 7.0 Continuity of Business in Emergency Situations

7.1 Does the DFMS departmental unit have a contingency plan for continuing critical business operations in the event that access to data and core records is interrupted?

7.2 Does the service provider have a contingency plan in place for disasters, interruption of communications services, loss of power, or emergencies?

7.3 Has the plan been vetted or approved by a client pool or other outside auditor or insurer?

7.4 Is there a disaster recovery plan in place? Does the contingency plan include an emergency shut down procedure and customer notification protocols? Is the plan accessible and schedule for periodic review? Does the plan identify individuals in the DFMS empowered to make decisions in emergencies?

7.5 Does the service provider have a current existing contract in place with a professional data recovery vendor in the event of an emergency?

7.6 Who is responsible for the costs of recovery should a disaster occur?

**8.0 Security**

8.1 What subcontractors or third parties have access to The Episcopal Church's data? How do these entities physically access the data?

8.2 Does the service provider have a robust firewall to prevent against external access from unauthorized users?

8.3 What procedures are in place to ensure that the contractor or vendor's employees cannot disseminate information to the wrong person?

8.4 What safeguards are in place to secure data from data corruption, data theft, or viruses?

8.5 What encryption methods are available and how are the encryption keys stored?

8.6 What notification processes are in place to alert the DFMS and the data managers to a security incident?

**9.0 Data Backup**

9.1 What are the Contractor/Vendor's standard backup procedures?

9.2 What backup storage devices are used? Are physical storage devices used and how are they managed?

9.3 What backup procedures does the DFMS have in place for the data that will be stored in this system? Will the DFMS be creating a periodic backup on its own servers and/or utilizing remote storage?

9.4 Where are the backup data physically stored? How can it be accessed? Does the service provider use a third party vendor for off-site storage?

**10.0 Accountability**

10.1 What other DFMS departments are affected by the new or revised system and have they been consulted about data retention requirements?

10.2 Who are the DFMS employees responsible for the implementation and maintenance of the system and for carrying out retention policies?

10.3 Has the decision making and auditing process been defined? Has a member of the DFMS staff been designated to monitor the system's audit trail? Has this information been documented with DFMS's Records Management Office?

*ver-gam_06/15/2011*

May 1, 2009

The following is a true copy of a Resolution adopted by the Executive Council at its meeting on April 20 – 22, 2009 in Portland, Maine, at which a quorum was present and voting.

*Resolved*, That The Domestic and Foreign Missionary Society adopts the "Records Retention and Management Policy," as approved by the Board of Archives and the Audit Committee and hereafter amended by the Board of Archives and the Administration and Finance Committee, and directs that the Society's employees follow the policy and the standard retention and disposition procedures developed from it as they apply to the Society's records and electronic communication.

**Explanation**

In response to a request for the development of a standard records retention policy for the DFMS by the Board of the Archives in 2007 and the Audit Committee of Executive Council in 2008, the Archives has prepared this policy proposal. In addition to these two bodies, the policy was circulated, reviewed, and revised to incorporate the comments of ECC management, in-house counsel, and professional peer reviewers. Effective policy and standard practice in the area of records retention, particularly for electronic records and email, has increased significantly in the past few years in response to the requirements for transparent business practice, cost effective response to legal discovery, management of corporate information assets, and Sarbanes-Oxley requirements for controls over electronic communication affect both the private and nonprofit sectors.

Compelling reasons exist for adopting an official retention policy for the Society's records at this time. Up to this point, DFMS retention practices have been largely advisory. Lacking endorsement by appropriate corporate bodies, records retention has been unevenly practiced. Many employees have interpreted retention recommendations as optional. As a result, the Society can not claim to have uniform retention standards or a common set of understandings and practices about what is permissible or prudent record keeping. This confusion exposes the corporation to unnecessary financial risks, legal liabilities, and costs associated with information loss. Adoption of a corporate retention policy is a prior step for the Archives before it invests in an enterprise-wide software solution to manage electronic records and implement retention guidelines.

Gregory Straub

The Rev. Dr. Gregory S. Straub
Secretary of the Executive Council and
The Domestic and Foreign Missionary Society
of the Protestant Episcopal Church in the United States of America

a&f 096

THE EPISCOPAL CHURCH

THE DOMESTIC AND FOREIGN MISSIONARY SOCIETY
OF THE PROTESTANT EPISCOPAL CHURCH IN THE UNITED STATES OF AMERICA

FOUNDED 1821 ▪ INCORPORATED 1846

June 30, 2011

The following is a true copy of a Resolution adopted by the Executive Council at its meeting from June 15 – 17, 2011 in Linthicum Heights, Maryland, at which a quorum was present and voting.

Resolved, That the Executive Council approves as a supplement to the DFMS Records Retention Policy, which was adopted April 20, 2009 (AF-096), the Guidelines for the Selection of Software for Records of The Episcopal Church as a standard for implementing systems used to manage the electronic records of the Domestic and Foreign Missionary Society and the General Convention, and requests that the purchase of new software systems or services affecting the records of the Society and General Convention be made after the required consultations as provided in the DFMS Records Retention Policy.

**Explanation**

These guidelines take the form of a set of questions that should be used as a tool to employees and agents of the DFMS and General Convention in purchasing and deploying computer software systems or services that hold the records of The Episcopal Church. The goal of the guidelines is to ensure that software systems comply with industry standards and the Society's policy for retention of data for legal, administrative and historical purposes.

This policy has been reviewed by management and information technology staff of ECC. The Board of Archives reviewed and approved these standards at its meeting on January 28, 2011 for submission to Executive Council.

Gregory Straub

The Rev. Canon Dr. Gregory S. Straub
Secretary of the Executive Council and
The Domestic and Foreign Missionary Society
of the Protestant Episcopal Church in the United States of America

gam 011