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

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