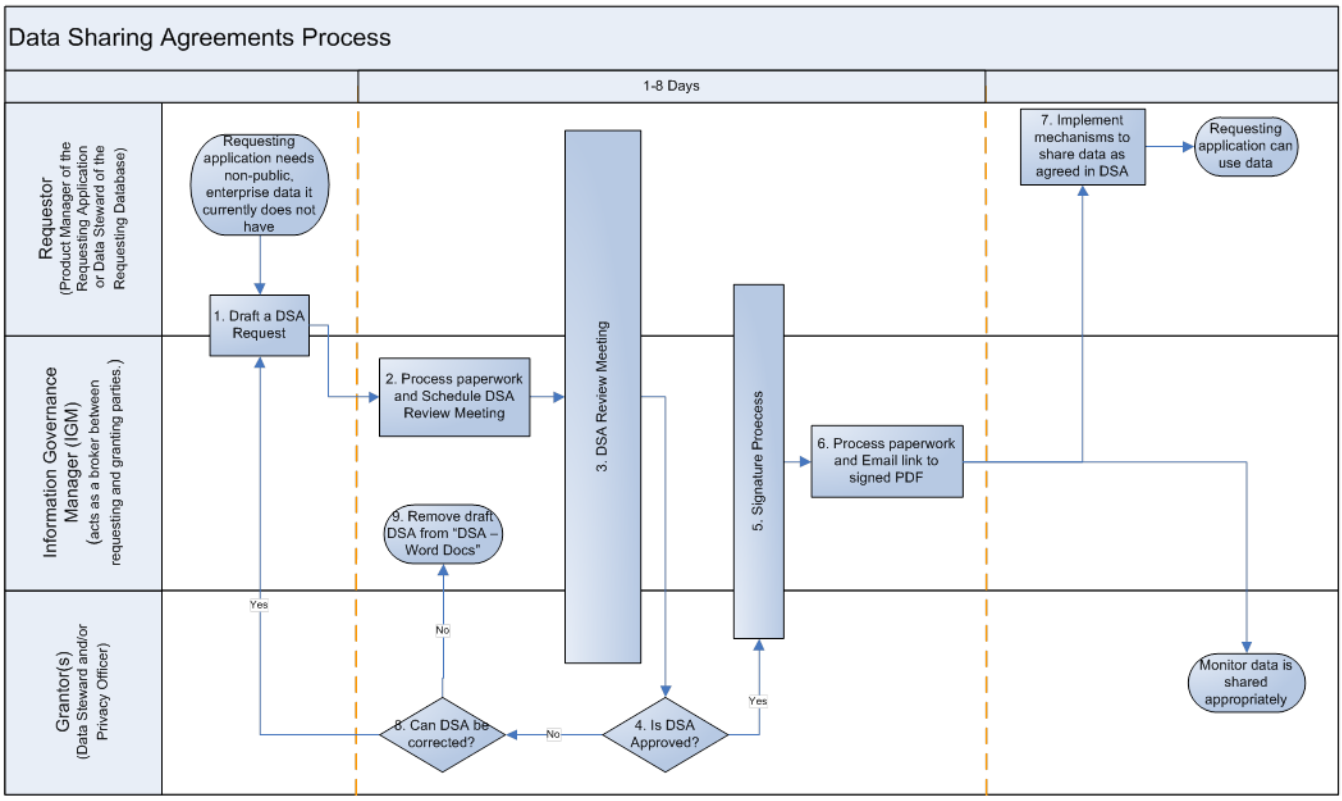
# Creating or Modifying a Data Sharing Agreement (DSA) Process

Created: April 1, 2008
Last Updated: March 17, 2011




## *Background Information:*

Data Stewards are responsible to ensure their data is used properly. A DSA is created when an application (or a repository) requires the use of a Data Steward's data. The DSA formalizes the intended use of the data, the specific data being shared, who will have access to the data, and describes the mechanisms for sharing this data. Generally an application will have one DSA for each Data Steward involved.

The Church Data Privacy Office is responsible for ensuring all personal information shared with other entities or affiliates comply with the Data Privacy Policy, Global Privacy Policy (notice provided on websites), and Data Privacy Statement. In addition, when personal information is shared with non-affiliated third-parties, the Data Privacy Office verifies the appropriate external data sharing agreements have been signed and are in place.

## *Process:*

1. The Requester owns this step and should initiate contact with needed resources to help fill out the DSA Template. Product Managers, Project Managers, Database Engineers, and the Information Governance Manager (IGM) are typically needed in drafting a DSA Request. If a DSA already exists, then the existing request found on the DSA-Word Docs website should be modified rather than creating a new one (please turn on "track changes" when modifying so that the changes are easier to review). This step is final when the IGM has a completed request.

2. The IGM initiates process paperwork and schedule the Review Meeting:
    a. Create a Remedy ticket under the name of the Requestor (Product Manager/Data Steward) to track progress of the DSA. Ticket data will be used to report on the speed DSAs are flowing through stages 2-6 of this process – the stages where the users doesn't drive the timeline.
    b. Documents the Data Domains and Data Stewards in the DSA request, and assign and document the DSA # if this is a new request.
    c. Upload the proposed DSA to the DSA – Word Docs website.
    d. Sets the status to "Draft" and fill in the other property data.
    e. Schedules a Review Meeting (step 3) with the requestor, the granting data steward, and the Privacy Officer of needed including the date, time, and place of the meeting, as well as the name and location of the DSA in the email (or attaches the DSA to the email). Meeting methods are scheduled in this order: face to face, tele-presence, meetingplace.
    f. Update the remedy ticket with meeting information.

3. The DSA Review Meeting ensures all parties agree on the specifics of the Data Sharing Agreement and identifies potential problems or shortcomings. A typical meeting will discuss the following:
    a. The requestor describes the business purpose of the requesting application (or repository).
    b. Review the specific data that is being requested and why it is needed.
    c. Review the sharing mechanism.
    d. Review the audiences and the access each will have to the requested data.
    e. Ensure the DSA documents these decisions. If not, the DSA should be modified to meet the stakeholder's expectations (if possible, these modifications are made in the meeting).

4. The granting Data Steward and/or Privacy Officer approve or reject the DSA. The decision must be unanimous if more than one approver is involved.

5. Various factors determine the type of signature process that may happen here. This may be electronic signatures, verbal approvals, email approvals, or it may be pen and paper signatures. The IGM will give direction on the methodology according to the Data Steward preferences and the availability of participants.

6. The IGM updates process paperwork and emails a link to the approved PDF:

7. Requestors implement the method to share the data abiding with any special conditions documented in Section D of the DSA.

8. If the request is not approved, the Data Steward and/or Privacy Officer determine whether the request is rejected due to insufficient information or due to the request being materially inappropriate. If the rejection is due to insufficient information, the Data Steward should communicate this to the Requestor. The Requestor then repeats the process starting at step 1 to ensure all aspects of the DSA meet the needed requirements.

9. If the request was rejected, the IGM updates process paperwork:
    NOTE: If the Requestor wishes to appeal the Data Steward's rejection, the Requestor should work with the IGM to determine the escalation path to pursue.

## *Defining Roles:*

### Requestor: Product Manager and/or Program Manager for Requesting Application

The business contact for the requesting application should be a party with a long-termed vested interest in obtaining the data and a representative of the project team from the requesting organization; typically these should NOT be ICS technical representative. These persons also perform most of the drafting and processing of the Data Sharing Agreements.

### Information Governance Manager

Responsible for documenting the sharing of data across departments and assuring that best practices are followed. This person acts as a broker between the Requestor and requesting Data Steward, facilitating the exchange of information and helping each party meet their needs within IT policies and principles for information governance.

### Data Steward for Granting Application

The person designated by the CIO and approved from within the granting department, and is responsible to:

a. Ensure proper access to and use of the data.
b. Ensure the quality, completeness, and accuracy of the data.
c. Provide descriptions, classifications, and handling requirements of the data. (See Information Classification and Handling Policy).

### Data Privacy Office

The Data Privacy Office is part of the Intellectual Property Division. The Data Privacy Office has the responsibility for all privacy matters of the organization and is responsible for developing and implementing data privacy policies and procedures designed to safeguard personal data collected and used by the organization in compliance with applicable data privacy laws and regulations.

(To see more detail within this process, select the text portion of this document (not the picture), right-click and choose “Font”, under “Effects” click the “Hidden” box twice, and click “OK”)