How to Create a Defensible Disposition Strategy

Organizations have more information to manage today than they have ever had in the past. The good news is that our use of paper has declined but, on the flip side, our use of email and electronic documents has increased. While the simply "keeping everything" may seem the natural thing to do, it is not the best information management strategy for an organization. A few of the reasons for not keeping everything include the organization will pay to store valueless information, you will have unnecessarily large volumes of information to search through when looking to retrieve information, e-discovery and freedom of information risks, and over-retention of personal information is contrary to privacy legislation.

Some organizations provide little guidance to their users regarding the disposition of information, often resulting in the over-retention of information or inappropriate deletion of information. In most cases, this means there are duplicate documents and data stored in multiple repositories. We need to subject the unneeded, duplicated and expired information to consistent, repeatable and defensible disposition. In short, bring our information under control.

A Defensible Disposition Strategy is a part of the overall Information Governance in place in organizations and a natural stage of the information lifecycle. The defensibility comes from the consistency, transparency and predictability of the information disposition, implemented in context of legal and business compliance.

Step 1: Identify Your Data Disposition Targets

To determine what to target for disposition, it is important to assess all your information and to understand the objectives that you are trying to accomplish by disposing it. At this stage, it is important to have the participation of key stakeholders such as legal, compliance, IT and senior management. Instead of starting by looking at the oldest information, which may seem to be the most logical, it may be more effective to look at the newer information to get it under control first. You should also review your records policies, retention schedules, and if you have a disposition policy, it should also be reviewed and updated if necessary, before you target and disposition of information.

AIIM Tip

First thing to do is to review your records retention schedules and gain an understanding of what you must keep and what must be discarded. Next, you should review the regulatory, legislated and business requirements for keeping that information. Do not forget to check for any legal holds that may be active in your organization. If your organization has a disposition policy, this should also be reviewed. Keep in mind that there may be departments that may decide to maintain records longer than indicated in your retention schedule: If that is the case you should obtain the business reason for maintaining the records longer and then seek approval from the legal department first. If you do not have a disposition policy, you should either develop one or make sure the disposition of information is covered in your records policies and procedures.

An effective disposition program really begins at the point the records and information are created. Applying appropriate metadata during the creation process will greatly aid the efficient and accurate identification of records and information to be disposed.

For more information

- Creating a Culture of Compliance: Defensible Disposition
- Information Governance Best Practices Webinar – Why Implement a Defensible Deletion Policy
- Push the Delete Button with Confidence
- Content Analytics: Automating Processes and Extracting Knowledge
- Frequently Asked Questions about Records Scheduling and Disposition
- Defensible Disposition in a Nutshell – My AIIM Talk
- Kahn's 8 Steps to Defensible Disposition Nirvana

Step 2: Establish a Disposition Strategy for Working Documents

Allow employees to save working documents in a searchable, centrally managed and controlled repository. Working documents in this context are short-term transitory records that employees need to do their jobs and be productive. These documents should be deleted as soon as they are no longer needed. Alternatively, they may be automatically deleted after an established time period such as two or three years.

AIIM Tip

Talk with the line of business people in your organization. Gain an understanding of how they use the information and what part that information plays in the business processes.

For more information

- The Good, the Bad, and the Ugly of Defensible Disposition
- Defensible Disposal: You Can't Keep All Your Data Forever
- Defensible Disposition of Structured Data
- 'Chucking Daisies' or How I Learned to Love Defensible Disposition
- A Quick Course in IT Asset Disposition (Infographic)

Step 3: Identify Your Disposition Strategies/Tactics

Before you begin to discard information, it is important to give some thought to developing strategies for the disposition of information. Remember, just deleting everything and starting fresh with a clean slate is not the approach to take. With any approach you adopt, there will be benefits and risks. The idea is to select the strategies that will best serve your organization and produce the results you want. Some of the strategies you may consider:

- Information governance team (legal specialist) endorses the disposition process
- Establish simple time-based Disposition Policies for working documents and other transitory information
- Meet with users and manually review their files together and delete those that are scheduled and meet the retention periods.
- Identify those in the organization who are in the top 5% of storage use and work with them to reduce the amount of storage they require.
- Delete emails based on rules.
- Have the IT department use monitoring and crawling tools to identify records which have met their retention.
- Migrate from one system or file share to another and only take the current or business pertinent information to the new system.
- Identify groups of records that are alike (i.e., all invoices prior to a specific year).

AIIM Tip

There is not 'one' correct approach to disposition of records that fits all organizations. It is important to consider your organization and its needs as well as any regulatory or other legal rulings that you must adhere to. Keep in mind that disposition is not a one time event. It is something that must be addressed on a continuing and systematic basis.

For more information

- Implement a Defensible Disposition Strategy to Manage Risk and Control Costs
- Manage Costs and Risk with Defensible Deletion
- Developing a Data Disposition Strategy
- Defensible Deletion
- Getting to Defensible Deletion

Step 4: Determine Your Technology Plan

Information governance technologies ensure the information is reliable. Technology plans will provide protection against spoliation of evidence for legal holds. This is not just about deletion upon expiration but making responsible decisions that reflect the value of the information in the organization. The technology plan will enable you to make effective use of technology to assess and dispose of the information in your organization.

AIIM Tip

Remember that there is no one tool. You may need to use a variety of different tools and technologies as well as techniques to dispose of the information in your organization. It is important to understand that the practical and technological paths need to be aligned with the disposition policy. It the system fails, it means we must do an even better job at integrating the conceptual with the people and technology never losing sight of the business and legal environment.

For more information

- Developing your Assessment Plan for Defensible Disposition
- Strategic Technology Plan
- Recommended AIIM Vendors who provide information governance technologies
- Automation Should Get the Job Done and Be Defensible in Court
- The Impact of Incorrect Training Sets and Rolling Collections on Technology-Assisted Review (TAR) and Defensible Disposition
- Evaluating automated approaches against records management principles

Step 5: Develop and Execute the Disposition Plan

You have reviewed the information you have in your organization and understand the requirements for keeping the information. The technologies and techniques to disposition the information have been identified. You know the impact that will be felt in the organization. Now is the time to bring this all together and develop a roadmap for disposing of the information.

Your roadmap may contain the following:

- Identify the records or data to be destroyed
- Gain Business approval to destroy
- Check for Legal holds (or other types of holds – audit, tax, etc.)
- Remove any records that are on hold
- Gain approval on final list
- Destroy records

AIIM Tip

The execution of the disposition plan may take some time, many months, or even years, to complete. Don't lose faith in your plan. Keep to the plan and execute it accordingly. As you execute the plan, you may want to review your policies again to make sure they are still applicable. After all, policies are governance documents that are subject to many changes in a work environment.

For more information

- Four Best Practices for the Defensible Disposition of Electronic and Paper Documents
- Electronic Records Management Training
- Information Governance Training
- Embrace Information Governance, The Time is Now
- Disposing of Electronic Records – It's About Time
- Disposing of Digital Debris