IRON
MOUNTAIN®

WHITE PAPER

THE ABCs OF DEFENSIBLE DISPOSITION

CONTENTS

03/ WHAT IS DEFENSIBLE DISPOSITION?

04/ WHAT IS A RECORDS RETENTION SCHEDULE (RRS)?

05/ WHY IS DEFENSIBLE DISPOSITION SO IMPORTANT?

06/ WHO SHOULD BE INVOLVED?

07/ WHAT ACTION CAN BE TAKEN?

08/ WHAT ARE THE BARRIERS TO SUCCESS?

WHAT IS DEFENSIBLE DISPOSITION?

With few exceptions, all information has an end-of-life point. At that time, a decision must be made to either destroy it or keep it for archival or data mining purposes, a process called document disposition. Key to the disposition decision-making process is an organization's legally defensible records retention schedule (RRS). Once a decision is made to destroy – or keep – records, the process must be conducted in a manner that is compliant with the organization's policy. This might mean secure shredding of paper records or degaussing of magnetic tapes. If records must be kept for a valid business reason, it could mean anonymizing them before moving them to a data lake.

Defensible disposition is making decisions about what data can be disposed of based on an official policy and then either moving it to a secure archive or destroying it in a compliant way.

> DEFENSIBLE DISPOSITION IS MAKING DECISIONS ABOUT WHAT DATA CAN BE DISPOSED OF BASED ON AN OFFICIAL POLICY AND THEN EITHER MOVING IT TO A SECURE ARCHIVE OR DESTROYING IT IN A COMPLIANT WAY.

WHAT IS A RECORDS RETENTION SCHEDULE (RRS)?

To manage official business records properly, organizations must have an official, authorized records retention schedule. Schedules are constructed by researching how long records need to be kept in all the jurisdictions in which an organization does business. In most cases, an organization's legal department is responsible for final approval of the research results provided by a vendor or an internal team.

The schedule lists the functions of an organization – such as HR, accounting, sales and marketing – along with all the groups or classes of records and examples of each. Records are defined as information that is created, received, and maintained as evidence and information by an organization or person in pursuance of legal obligations or in the transaction of business.

For each class of records, such as accounts payable and receivable or personnel, a retention rule is assigned based on regulatory, legal, and operational requirements that specifies the length of time the records must be retained. For example, the rule might require that records be retained for 10 years after creation or seven years after an event has occurred. In fact, some people prefer to call the records *retention* schedule a *destruction* schedule to discourage over-retention and promote disposition.

Organizations must also make policy decisions about how long data and information that is not considered official business should be kept, whether in paper or electronic format.

RECORDS RETENTION SCHEDULES CAN TAKE MANY FORMS, BUT A SIMPLE ONE MIGHT LOOK LIKE THIS.

DOCUMENT	RECORD TYPE	RETENTION PERIOD	RETENTION MEDIUM	POST-RETENTION DISPOSITION
Receipts	Original or Digital	Five Years	Paper/Digital	Destroy Upon Expiration
New Hire Forms	Original Copies	Seven Years After End of Employment	Paper/Digital	Destroy Upon Expiration
Legal Files	Original Copies	10 Years	Paper	Scan and Archive
Client Meeting Notes	Original or Digital	10 Years Following Closure of Client Account	Paper/Digital	Destroy Upon Expiration
Deeds, Mortgages	Original Copies	Permanent	Paper	Scan and Archive 10 Years After Signing
Expense Reports	Concur Database	Three Years	Digital	Permanent Erasure

WHY IS DEFENSIBLE DISPOSITION SO IMPORTANT?

WHILE MOST ORGANIZATIONS HAVE A RECORDS RETENTION SCHEDULE, PEOPLE OFTEN HESITATE TO DESTROY INFORMATION, THEREBY FOSTERING A KEEP-EVERYTHING CULTURE THAT FRUSTRATES DISCIPLINED RECORDS MANAGEMENT. RELUCTANCE TO DISPOSE OF RECORDS IS TYPICALLY CAUSED BY ONE OR MORE FACTORS:

- People may not want to accept responsibility for destroying data that may be needed later, no matter how remote the possibility may be.
- It may be difficult to determine the dates of some records for disposition purposes.
- People unfamiliar with the details of managing electronic content may fear that their actions could have unintended consequences.
- Mystery data, often obtained through a merger or acquisition, may not be accounted for in the RRS.
- Sometimes it's simply easier not to make a decision.

A new consideration has emerged in recent years that organizations must also address: the growing role of data analytics in enhancing organizational efficiency and competitive advantage. Analytical processing may require keeping records and data on the retention schedule longer than specified for historical analysis.

Despite people's natural reluctance to destroy anything, there are a multitude of reasons why adhering to records retention rules is important.

- In many countries, provinces, and states, data privacy laws dictate that records containing personally identifiable information (PII) must be destroyed after they are no longer needed. Substantial fines can be levied for noncompliance.
- Keeping records longer than required can expose organizations to unnecessary litigation or Freedom of Information Act request exposures and costs.
- With security breaches on the rise, over-retention risks making more information vulnerable to falling into the hands of bad actors.
- Keeping everything simply because it's easier than throwing it out actually makes data analysts' work harder. Disposing of low-impact information reduces noise and enables them to concentrate on the most useful data.
- As most records age, their value decreases, while the risk of keeping them increases.
- The bottom-line cost of carrying records for longer than required hits business units in the form of administrative burdens, consumption of valuable real estate, and costs for storing records offsite.
- Ensuring the authenticity of information as it is shared and used becomes more difficult over time.
- New regulations in the European Union and elsewhere include right-to-be-forgotten provisions that require organizations to locate and remove all information associated with an individual upon request, regardless of where or how it is stored. Proactively disposing of such information makes compliance with these requests easier and reduces the risk of noncompliance.
- Destroying paper originals after they are imaged removes the risk of unnecessary duplicate copies being created. In most cases there is no need to keep the paper version if quality control standards have been met.

INFORMATION GOVERNANCE SHOULD INCLUDE IT, LEGAL, RISK, COMPLIANCE, RECORDS/ INFORMATION MANAGEMENT, DATA ANALYTICS, SECURITY AND KEY BUSINESS UNITS.

WHO SHOULD BE INVOLVED?

In an ideal scenario, an organization should have or create an information governance body to guide the disposition decision-making process. The committee should include representatives from IT, legal, risk, compliance, records/ information management, data analytics, security, and key business units. The goal is to come to a consensus on how to execute defensible disposition across the enterprise, keeping in mind the possible secondary uses of information once its original purpose has been fulfilled. Legal and compliance professionals should be involved at every stage.

Establishing a policy can be a delicate task, as people are often fiercely protective of information. Culture can also be a barrier to the advancement of information governance if people tend to hoard information or equate data ownership with status. These barriers can only be knocked down with high-level executive support, an essential first step in the disposition process. Compliance and legal professionals can help explain to stakeholders the risks involved.

The COVID-19 pandemic introduced new complications in disposition decision-making and execution because employees were forced out of offices. The records they left behind may be well past their eligible destruction date and will require immediate action once offices reopen. Attention will also need to be paid to data created on devices the organization doesn't own, an issue that is likely to be ongoing as more people work all or part of the time from home in the future.

WHAT ACTION CAN BE TAKEN?

The first step in establishing a defensible disposition policy is the same as the first step in implementing an information governance plan: Find out what you have. This includes data in print, on devices, and in the cloud. Create a benchmark for progress by documenting the location and volume of both paper and digital records. Categorize these records and apply meta tags with the greatest level of detail possible.

A computerized data catalog is useful for classifying digital records; paper documents can also be tagged through printed labels and consolidation into boxes with similar records. Be prepared to apply technology wherever possible, since information may be on everything from PC hard drives to smartphones and USB sticks.

Metadata tags are an essential part of records retention. They enable people to quickly find the information they need and to group like records. Tagging also permits automated operations to be performed at scale, such as a high-volume erasure or archive. Unfortunately, most organizations are not disciplined about applying meta tags. This hinders their ability to effectively analyze information because they can't find the information in the first place.

Records retention is highly dependent on metadata to identify actions to take throughout the information lifecycle. Ideally, data should be tagged at the creation stage, but tags can be applied and modified at any time. Use clear and consistent naming conventions and apply tags at specified points, such as when data enters a workflow or is submitted to offsite storage or archive.

Use the audit process to root out information that is clearly past its retention expiration date, as well as redundant, obsolete, and trivial (ROT) data, which often accounts for 30 percent or more of the data the organization has. This process sounds involved — and it is — but it only needs to be done once. When coupled with a disciplined approach to ingesting new data, records disposition becomes self-sustaining.

WHAT ARE THE BARRIERS TO SUCCESS?

DEFENSIBLE DISPOSITION INITIATIVES INVARIABLY ENCOUNTER SOME OBSTACLES, BUT ANTICIPATING THEM CAN MINIMIZE THEIR IMPACT. HERE ARE SOME OF THE MORE COMMON IMPEDIMENTS.

EVENT-BASED RULES

Unfortunately, not all retention schedules can be pegged to the date a record was created. Event-based retention rules start the clock ticking when something happens, such as a contract being signed, an employee being terminated, or a customer closing an account. The best solution is programmatic, meaning that the software that records the event fires off a notification to the enterprise content management system to start the countdown. Such modification is straightforward with most modern applications but may not be so easy with older programs. Where automation is not possible, periodic content reviews and even manual audits may be necessary. It may also be possible to convert some events that have a low risk of litigation to a soft create date that permits automated disposition.

DECISION PARALYSIS

Faced with a detailed, multipage retention schedule covering hundreds of content types, some employees will be so overwhelmed that they will choose to do nothing at all. A good strategy is to create a simpler big-bucket retention schedule with fewer categories that is organized by a few departments or roles. While this approach may result in some records being retained beyond their specified destruction deadline, it will encourage employee compliance and ultimately make disposition more effective.

INFORMATION HOARDING

When notified that their email records are going to be deleted after six months, some employees may resort to tactics that create risk, such as archiving their inboxes to removable USB drives or, worse, forwarding them to personal email accounts. An effective remedy is to provide safe longer-term storage of email archives to folders that are invisible on the corporate network and that are scrubbed every two years instead of every six months. Employees should also be trained how to download and tag attachments rather than leaving them in their mail files.

DARK DATA

Most large organizations have records that no one can identify or remember why they were created. These may be in physical boxes or on software applications that were installed by people who have since left the company. The information governance committee should develop consistent practices, such as sampling, manual inspection, or offsite storage with scheduled destruction, for dealing with this mystery data.

CONFLICTING DATA

It isn't uncommon for organizations to have a half-dozen different records for the same customer, each with slightly different spellings, addresses, and phone numbers. The audit process is a good time to uncover these records and clean them up. Cloud-based automated tools incorporating machine learning are making this process, which was once mostly manual, considerably less painful.

DATA ANALYTICS

Big data and analytics tools have made historical data useful again. Data scientists and business intelligence analysts often fold years of records into their forecasting models to help spot trends. Much of this information may be past its expiration date. Work with your IT organization to provide a free-form data lake for this kind of activity, making sure that data is first anonymized by removing personally identifiable information. Such details are usually not necessary for data science purposes anyway.

EQUIPMENT DISPOSITION

The most meticulously planned records retention strategy can be undermined if old IT equipment is disposed of haphazardly. Many people don't know, for example, that erasing a file from the disk only removes the pointer from the directory but deletes little or no data. Sensitive information stored on USB devices, cell phones, and even old printers can be deciphered by cybercriminals. Any equipment that is to be resold should be thoroughly scrubbed by a professional firm. A certified data destruction vendor with secure facilities and certified destruction practices provides protection against legal and regulatory action.

CONCLUSION

It's time to stop hoarding data and instead treat it like any other asset that has outlived its usefulness. A records retention schedule, combined with a disciplined approach to disposition, cuts down on clutter, eliminates duplication, and makes organizations leaner, faster, and more decisive.

FOR NEWS, INSIGHTS AND INFORMATION MANAGEMENT BEST PRACTICES, PLEASE VISIT IRON MOUNTAIN'S KNOWLEDGE CENTER AND INFOGOTO BLOG.

KNOWLEDGE CENTER:
WWW.IRONMOUNTAIN.COM/RESOURCES

BLOG:
WWW.IRONMOUNTAIN.COM/BLOGS

800.899.IRON | IRONMOUNTAIN.COM

ABOUT IRON MOUNTAIN

Iron Mountain Incorporated (NYSE: IRM), founded in 1951, is the global leader for storage and information management services. Trusted by more than 220,000 organizations around the world, and with a real estate network of more than 85 million square feet across more than 1,400 facilities in over 50 countries, Iron Mountain stores and protects billions of information assets, including critical business information, highly sensitive data, and cultural and historical artifacts. Providing solutions that include secure storage, information management, digital transformation, secure destruction, as well as data centers, art storage and logistics, and cloud services, Iron Mountain helps organizations to lower cost and risk, comply with regulations, recover from disaster, and enable a more digital way of working. Visit www.ironmountain.com for more information.