# INFORMATION GOVERNANCE 101:

# GETTING RID OF THE CONTENT YOU DON'T NEED

A GUIDE CREATED BY aiim

# INFORMATION GOVERNANCE 101:

# GETTING RID OF THE CONTENT YOU DON'T NEED

## INTRODUCTION

Is your organization an information hoarder or an information purger? For years we have been accumulating information in various forms from paper to electronic documents and social media content such as blog posts and tweets. Many organizations think that they have to keep all of this information. What they fail to realize is that not all information is equal. By keeping information that isn't needed and not following an information governance plan, organizations put themselves in jeopardy. Proper information governance includes getting rid of information that no longer has any value to the organization. Simply put: you don't need to keep it all – and you shouldn't.

Accumulating information in our information repositories is a continuing (and continual) process. But, there isn't a prize for being the organization with the most information. However, there is a "prize" for organizations that don't take their information governance seriously by discarding information that has served its useful life. The "prize": increased storage and maintenance costs at a minimum to possibly exposing your organization to unnecessary discovery costs (and potential risk) during litigation. Make no mistake about it, purging documents is a difficult and time-consuming task, but one that is very worthwhile. When we do not take the time to review and purge unnecessary records, we lessen the value of the information that we do keep.

The information governance policy that you have implemented in your organization gives you the ability to throw content away as long as you do it in accordance with the guidelines established by your policy. We have mentioned "Information governance" three times already. So, what do we actually mean? Information Governance is "The establishment of enterprise-wide policies and procedures and the execution and enforcement of these to control and manage information as an enterprise resource." Inherent in this definition is the understanding that an organization must manage its information from the time it is created until its usefulness to the organization is over – and that it's OK to remove it from an information repository.

# DISCARDING INFORMATION

In many organizations, the reason so much information accumulates is because we like to retain information and fail to dispose of it when its business, legal, or regulatory value has been expended. We are often afraid to delete unnecessary information because it might be needed at some time in the future. How many times have you kept something "just in case"? Individually, this can lead to extra paperwork overloading our desks (and digital files) and be an annoyance. Up a level, keeping extraneous information can be detrimental to the organization. With the introduction of regulations like the Federal Rules for Civil Procedures (FRCP), organizations for the first time are recognizing the potential of seeing their top-level executives sent to prison because their organization either did not have information governance in place, or did not follow it. It is not enough to document the policies for managing your information; your organization must implement and enforce them. This means ensuring that everyone from the top to the bottom of the organization is aware of them and understands their role. Everyone is an information steward.

You must involve the right people in the development and implementation of information governance. This includes representatives from IT, legal, line-of-business, records management, and compliance. Each representative brings to the effort a unique perspective that helps frame information governance for your organization. IT sheds light on the technical capabilities of the organization's infrastructure to ensure the information is managed appropriately. The legal department shares its knowledge of relevant industry regulations and business laws of how records must be maintained for your organization. Records managers translate the regulations into records practice terms to ensure that the compliance department can enforce the governance plan.

# GETTING STARTED

Let's start by reiterating a critical point: it is okay to discard information if you have the appropriate policies and procedures in place as a part of your information governance. Governance must encompass both paper assets and all of your electronic information, network drives, employee technology (i.e., laptops, tablets, smart phones, storage devices and as if it were not complicated enough – in the cloud!), etc. To describe this mountain of digital "stuff," AIIM uses the term "Digital Landfill." When I think of our (and I do mean "our" because I am as guilty as the next person for keeping documents in multiple places) digital landfills; I always picture information in a huge pile with people scurrying around trying to keep from having an information avalanche – you M*A*S*H fans might remember the episode with a huge pile of garbage.

Discarding information can be fairly easy if you have good information governance in place and everyone in the organization knows what should be kept and what should be discarded. The technology is available for your organization to use to help discard the paper and electronic documents that have been useful to the organization but are not as useful as it once was.

When we clean our garages or reduce the clutter in our lives, most of us use the rule of thumb that if something has not been used for three or more years, it should be discarded or recycled. Unfortunately, that rule of thumb doesn't work for an organization's information. Instead, you need to use your established records retention schedules to guide you in what you can discard. One of the initial tasks you should complete before discarding any information is to review the retention periods that have been established for your information. This means getting a copy of your records retention schedule and verifying the length of time records are to be retained. You should check with your legal department or legal advisor to make sure the period of time is appropriate for the industry you serve. The retention period should be based on local, state, and federal government requirements as well as good business practice. A general rule of thumb – this one IS OK to use – is to use the retention period that is the longest to ensure you will best meet the requirements. The records retention schedule should be reviewed and approved by senior management.

> Proper information governance includes getting rid of information that no longer has any value to the organization. Simply put: you don't need to keep it all – and you shouldn't.

# NOW THE FUN STARTS

Armed with your records retention schedule, it is now time to roll up your sleeves and begin to work on your digital landfill. Similar to the garage-cleaning exercise mentioned above, you may want to view this task as review, discard, and transfer the content as you assess the information you have. Just as not everything must be kept, we also do not want or need to discard everything either.

During the assessment phase, you will begin to review your content to determine the retention periods that have or will soon be ending, which means the information is no longer valuable to the organization and is no longer needed. This signals that it is time to take action and dispose of the information in accordance with the established methods as identified on the retention schedule or transfer it to the archive if there is some historical or other value for maintaining the information.

You need to determine which of two basic approaches (day forward or historical) you'll take as you assess your information with an eye to getting rid of all that is no longer needed. With the day forward approach, you declare a date as your starting date and implement the destruction policy from that day forward. This means you will not go back into your repositories and discard information dated prior to that date. Any new information or documents will be subject to the retention and destruction policy. A slight variation to this approach is to still use the day forward approach but when a record in the repository is used, it is then subject to the destruction policy. This is a little less labor intensive than the historical approach, which is to go through all the records in the repository and dispose of those that meet the retention guidelines you established. As you can imagine this is a VERY labor intensive process and will take a long time to complete. This becomes a very complex project when you consider all the locations where you store information.

> It is not enough to document the policies for managing your information; your organization must implement and enforce them.

If you want to see results quickly, one of the first things you can do is to de-duplicate your information. In other words, identify and delete all of the duplicates or multiple copies of identical documents and keep only the official record. Be sure that the record is an identical duplicate of the original or official record. Even one minor marginal notation makes the document a new original or official record. Don't forget that duplicates can hide in many locations such as shared drives, portable drives, laptops, personal drives, email services, content management systems, etc.

As you are assessing your documents or information, you should identify the information that can be destroyed and that which you should transfer to a permanent archive. To determine this, you must consult the records retention schedule and assess the overall value of the piece of content for the organization. The assessment you are doing determines how much junk or unnecessary information you have and how much constitutes a true record that has continuing value for the organization. You will find that there is going to be some information that is not easy to identify for destruction or transfer and preservation. To speed the process, identify and set aside that information so that the appropriate course of action to take with it can be considered at a later time.

> If you decide a record should be destroyed, it is important to have confirmation controls in the process that keep a record of the destruction of the record and who authorized the destruction as well as when it was destroyed.

When you decide to preserve information, determine the value the information brings to the organization. Typically, the value information has will be one of administrative, legal, fiscal, or historical reasons. If the information has one of these values, it should be transferred to the archive and removed from the repository where the current records reside. In transferring the record, you should ensure that the integrity of the record is preserved and that it is sustainable. In other words, it should be stored in a format that is not dependent on technology to be able to display the document in the future. This may mean that you would need to convert the file to a sustainable format such as PDF/Archive or XML.

The IT department can be instrumental in helping to ensure that the electronic records have, in fact, been properly destroyed. If the records are in paper format, you have two options available to you. For records that are not confidential, you may want to consider recycling the paper. When you have records that are considered confidential, you should first have the records shredded – either on your organization's site or hire a reputable company to do the shredding for you. After the documents are shredded, you could recycle the paper shreds. Whichever method or the format of the information, electronic or paper, you choose to use, make sure you have a record of the destruction that describes what was destroyed, who authorized it, when it was destroyed, and the method of destruction that was used.

The policy you have defends your actions and what you intend to do and acts as a protection for your organization. However, you must follow it!

# BENEFITS

As we remember that what we set out to do is to dispose of information that no longer has legal, regulatory, or business value, we can begin to see that there will be many benefits to the organization as a result of our efforts to reduce our information footprint. The benefits of discarding information fall into three major categories:

**Reduce risks –** Keeping information too long can be equally as risky as discarding information. As long as you have information governance in place and are following the policies and procedures, you can and should delete information that is no longer useful or has value for your organization. With less information to sort through, you will be able to efficiently address legal and regulatory compliance issues when they arise. This means you will be able to address electronic discovery (e-discovery) in a more efficient and timely manner.

**Reduce storage space –** Just because everyone says that storage is cheap does not necessarily make it so. It costs money to store information on your network drives or in the cloud. By reducing your storage costs, your IT budgets can be used for strategic investments rather than for the storage.

**Reduce costs –** Another benefit of assessing your information is that you will gain a better understanding of the cost of information and how much it costs to manage it. You will be able to align people, processes, and technology to better enable your organization to handle the work it must do to generate the revenues that will return more profit to your shareholders.

# CONCLUSION

The information governance policies and procedures that you have developed for your organization give you the ability to get rid of information that no longer is needed or has value for your organization. The policy you have defends your actions and what you intend to do and acts as a protection for your organization. However, you must follow it! This means you must make sure everyone in the organization is aware of it and knows how to implement it in their daily work. Since everyone in the organization is an information worker, this means that everyone is also an information steward and is responsible for the reliability or trustworthiness of the information in the organization.

> Everyone is an information steward.

In addition to promoting your information governance and auditing against the guidelines to ensure compliance, it is also important to make use of the available technology. Content and records management systems have the ability to help you maintain records for the established retention periods. It is a good idea to make use of these features and to make sure that some notification exists to warn the information worker that information is about to be deleted prior to deletion. Another feature of technology that will help to further implement the information governance is the use of auto-classification and analytics.

Restore the value of your information by becoming an information purger and getting rid of the information that no longer has value to your organization. It is all right to discard information as long as it has met its usefulness with respect to legal, regulatory, and business value.

# ABOUT AIIM

Here at AIIM, we believe that information is your most important asset and we want to teach you the skills to manage it. We've felt this way since 1943, back when this community was founded.

Sure, the technology has come a long way since then and the variety of information we're managing has changed a lot, but one tenet has remained constant. We've always focused on the intersection of people, processes, and information. We help organizations put information to work.

AIIM is a non-profit organization that provides independent research, training, and certification for information professionals. **Visit us at www.aiim.org**.

**AIIM**
1100 Wayne Avenue, Suite 1100
Silver Spring, MD 20910
301.587.8202
**www.aiim.org**


Take your skills to the next level with AIIM's Information Governance training course.

**CLICK HERE TO LEARN MORE**