4 Things to Include in a Document Management Policy

This is an extra resource to go along with the original article:
ID Capture: Do's and Don't's

How Documents Should be Created

If you don't specify how your employees should create documents, you'll find a lot of inconsistency that leads to disorganization. Some employees may create new files from copies on their personal computers, while others go to the official template on the local server. Still others may prefer paper copies.

If you want a better handle on how data flows through your organization, you need to start by dictating how documents are created.

How Documents Should be Stored

Making sure that employees can find the information they need when they look for it is crucial.

A document storage policy should explain how files should be stored and organized, including the preferred file format, filing location, and how each file should be named or labeled.

Which Security Measures are Required for Each Document Type

Some types of documents need more security than others. How will your organization flag sensitive files and control who can access them? Include information about how both physical paper files and digital files will be protected and backed up.

How Documents Should be Deleted or Destroyed

Information should only be stored for as long as it's useful. Old files take up unnecessary space that you'll pay for one way or another, and old files can compromise your security unnecessarily. Decide how long files should be stored before they're deleted, and specify *how* they should be deleted or destroyed (such as shredding paper or deleting digital files off the server).