

## 1. Purpose of this Standard

The purpose of this standard is to set the guidelines for the differences between the various classifications, or formats, of files found in the management of information.

## 2. Risks of non-compliance

Some of the risks of not having, or not complying with these standards are:

- Files of different classifications are managed the same way, creating gaps in the management and distribution of files
- Security and permissions of different file classifications will suffer, creating incorrect access to highly controlled files
- Electronic files are managed as hard copies would be, creating a difficult to use structure
- Digital data will not be sufficiently integrated into the access and relationships to the electronic copies

## 3. Overview

There are four possible classifications of files in each category:

- Hard (paper) copy files
- Electronic (soft) copy published files
- Electronic (soft) copy modifiable files
- Digital only

Each classification has unique requirements surrounding security, access to files, use of files, and required workflows.

It is imperative that organizations understand the retention requirements for all categories and classifications of files, and removes unnecessary superseded data from circulation wherever possible.

## 4. Hard Copy only files

While there is a strong push to go purely electronic, not all industries can achieve this goal as regulatory government agencies or departments require hard copies to be created and stored as evidentiary information as part of submissions to such agencies or departments.

As a result, hard copies continue play a role in Document Management.

In addition, until all personnel, particularly those in the field and operations, are able to work in a purely digital or electronic environment, hard copies will continue to be required.

There are two main forms of hard copies, the original hard copy and the reproduced hard copy. The original hard copy is the paper copy that has been signed with a pen (referred to as a wet signature). This original hard copy is used to create an electronic published copy. The reproduction of an original

hard copy as a print or photocopy of the original hard copy, and is used when hard copies are required by consumers of the data.

Original hard copies should not be used by the general consumer of the data unless absolutely required, and in such cases, a tracking mechanism must be in place to ensure that the original hard copy does not get lost and that its location and those responsible for it are known.

All reasonable efforts should be made to reduce the amount of paper that is produced, since technology is now, more than ever before, recognized as the source of truth for data in the majority of its forms.

For all hard copies that are required for each particular industry, all possible efforts should be made to create an electronic format of each hard copy file. This allows for original hard copies that require hard copy retention to be kept in a secure, climate controlled when necessary, environment where misuse of the paper can best be avoided.

#### **5. Electronic (or soft) copy files – Published files**

All information that is contained in the form of a drawing or document that is required to be distributed should be created in a format not easily modified, such as Portable Document Format (PDF) files.

PDF files are mostly protected from misuse, while still allowing access to the content by the designated consumers of the information. PDF files should be derived from the signed or authenticated hard copies, or digitally signed electronic copies whenever possible, mitigating the effect unsigned content has on the consumer, such as acting on unapproved files.

PDF renditions are PDF files that have been derived directly from an unsigned modifiable file. These are appropriate for sending incomplete content for information only, but must be marked as such to avoid misinterpretation of use.

It is acceptable to scan cover pages that contain signatures and render the remainder of the document to better enable text searchable documents, but the signature page must be present within the file.

#### **6. Electronic (or soft) copy files – Modifiable files**

Modifiable files, due to the vast numbers of software applications, have the most differences between the different categories of files.

Modifiable file formats come in a great many types, with the most common being the word processing or spread sheeting applications and various CADD software.

The protection and control of modifiable files is paramount, and all efforts must be made to ensure that unauthorized modification to files does not occur. Chain of custody must be evident in the storage and access to the files, the workflows, and in the storage of these files within transfer platforms such as emails and File Transfer Protocol (ftp) sites.

The strictest of control is required for the modifiable drawing files, as these files are most often what are authenticated and issued for construction, and thus must be protected from malicious or accidental disruption of the content contained within. This is most commonly an auditable requirement.

Modifiable files of Facility Documents must also be strictly controlled, in a similar manner to drawings, as these files are required to be updated over the operating life of the facility or asset to which they pertain. Lack of control will allow for uncontrolled duplication or potentially incorrect technical content, which can then adversely affect the fabrication/construction/installation, commissioning or operation and maintenance of a facility, or parts therein.

Facility Drawings and Documents also most often play a role in concurrent engineering, or concurrent projects, and as a result are exposed to a lot of movement. Expert tracking is required to ensure that the integrity of these files is maintained, particularly when concurrent activities are being executed.

The modifiable files of Project Documentation will be suited to the culture and of the organization.

Corporate Governance documentation modifiable files also require a high level of control to ensure that files do not get modified based on individual's preference.

Modifiable files can also act as an original in the event that a digital signature is embedded. Digitally signed modifiable files are to be treated in a manner similar to the hard copy original, and should never be the file that is used for subsequent revisions. Modifiable originals must be stored securely with evidentiary structure that is capable of demonstrating that they have not been tampered with after, subsequent to signature. This applies to files modified in all software applications.

For standards on the control of modifiable files, see DMC-DM-STD-012.

## **7. Digital Only**

Digital data can either be found in a database file, which may be extracted into a file format compatible only with the same or similar software application, or it can be digital only information used within the application, or to integrate with other software applications.

Some digital data can be exported into a spread sheeting application for manipulation. For example, metadata, which is defined as data about data, are pieces of information that pertain to a specific file that has been uploaded into a repository. A repository can be a simple software application that houses electronic files and has some simple capabilities, or it can be a complex system that allows for multiple actions and interactions, depending on the needs of an organization.

Digital data can be manually entered into a software application or spread sheeting tool, or it can be extracted from documentation into the system.

All efforts must be made to ensure that each piece of digital data lives in one system, and any other system that requires the data be integrated with that system. Digital data should not be entered into multiple systems, unless absolutely necessary due to poor integration capabilities of the infrastructure or applications being used.