1 Purpose of this Standard

The purpose of this standard is to provide details in the secure management of modifiable files. Security and chain of custody of these files is dependent on the purpose of the files, and on the content within the files. See DMC-DM-STD-022 for engineering sector specific modifiable file control (to be used in conjunction with this standard).

2 Risks of non-compliance

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

- Incorrect versions of modifiable files could be used for updates
- Files required to be modified by multiple groups/individuals are uncontrolled
- Multiple files of the same revision number may contain different content
- Confidential content or formulas may be unlawfully distributed
- Conflicts in content may occur due to multiple sources of input
- Security audits may result in dissatisfactory scores

3 Overview

The modifiable file component is the component that referees and controls the modifiable files of documents. This is the control needed to ensure the proper addition, deletion, and modification of content that is found in the published documentation.

Security of modifiable files is paramount to any organization. If the same file is modified by two different groups at the same time, it can create confusion and incorrect or conflicting content.

They must be protected from intentional and unintentional unauthorized modification. This means that they cannot be stored in a location that can be accessed by all personnel, and those who do have access must be properly trained in their management. It also means that they cannot be left as attachments to emails when the email is filed, and must be transferred to single points of contact whenever they are sent back and forth.

4 Modifiable File Requirements

4.1 General Documents

For most document's modifiable files, a lower level of security and control will suffice. A framework must be established to ensure modifiers clearly understand which file is the current version, so that further changes will be done correctly.

4.2 Financial Documents

Modifiable financial documents must be strictly controlled within the financial group to avoid undue changes or access to hidden formulas contained within the files. This may include financial information contained within the Purchasing groups' files, in which case they are to be strictly controlled by the Purchasing group.

4.3 Corporate Governance Files

The modifiable formats of corporate governance documents and templates must be controlled to the extent that the files must be formally requested. This ensures that all changes that are done to data that controls how an organization performs their work is monitored. Monitoring also entails the process of appropriate cross-functional review and adequate implementation of the changes.

4.4 Legal Documents

Legal documents could take many forms. It could refer to sensitive financial or special terms and conditions components of contracts or purchase orders, it could relate to contracts with employees or consultants, it could also pertain to confidential personal information as part of an investigation or claim. Absolutely all federal and other privacy acts must be adhered to. Chain of custody of these files is paramount. These files often contain content which cannot be modified by the general user, giving them access only to the portions which they may contribute to.

5 Control of Modifiable Files

5.1 Signing Out files

When any group or individual needs to modify a controlled file, they have to request the most recent version of the file from the appropriate Document Management group. If the file is available (it is not signed out to another group or individual) and the requestor has authorization to modify the requested file, then the file can be transferred to the requestor for use. It will always include a transmittal with clear instruction (i.e. files are signed out for modification, and strict chain of custody must be in effect).

Note that highly controlled modifiable files should not be sent to any other group other than the authorized Document Management representative. Document Management should be bound by ethics and must be trained to properly manage the chain of custody. There are very rare circumstances where a highly controlled modifiable file is sent to anyone else, but must be avoided if possible.

5.2 Files for Update

For the time that any group or individual has a modifiable file, they will have to continually send copies of those files in to the Document Management group at predefined issue stages. They are to be issued to, and received by, the Document Management group at all hard revisions, at a minimum.

The files are sent including a transmittal that clearly states they are for Update Only. The files are placed into the controlled area, and the files remain Signed Out.

Modifiable files sent for update must exactly match the signed published version of the document. This means that when they are submitted to Document Management as published, any quality issues that are found and corrected during the Publishing process, must be incorporated into the modifiable files.

5.3 Files for Sign In

Once the modifiable file is no longer needed, or if the modifiable file has been requested back by Document Management for any reason, the file needs to be sent on a transmittal that clearly indicates it is for Sign In.

This means that the group or individual no longer has the authorization to modify that file.

The group or individual must subsequently ensure that any file that has been signed in is either securely stored in a separate location, or deleted from any other location it was placed during modification.

If a previously signed in file is to be modified again, it must be requested from the Document Management group again. It cannot be assumed that the version that was Signed In is still the most recent and up to date version.

5.4 Files for reference only

Occasionally, modifiable files are sent to groups or individuals for reference only. Reference files may not be modified without prior written consent from the Document Management group.

5.5 Concurrent Modification

If a modifiable file is signed out to one group or individual, and another group or individual requests the same file, the initial modifier is asked to sign in the file to the owner. It is subsequently signed out to the second requestor. If the initial modifier is unable to sign the file in due to the activity schedule, management of both departments, or at both organizations (if external organizations are modifying files, are to establish priorities.

If an agreement on modification priority cannot be made, a controlled duplication of modification must be established. No revisions may be duplicated when in conjunction with a document number. Any temporary files must be merged together with the master file at all hard revisions.

Every movement of a modifiable file must be logged or if using a software system, the file must be uploaded and then downloaded again so the system knows to track the movements.

6 Basic Modifiable storage requirements

Files with the same security requirements must be kept together within a network drive structure, organized by simple groupings. Reference files that are embedded must be kept in a structure that will not change to ensure the integrity of the reference.

Files that require different securities must not be stored together in a network drive. Securities must be set by root folder, not by individual file.

Securities within software platforms must be by documentation category (See DMC-DM-STD-003 for classification definitions).