Last updated November 2015

M-FILES QMS - 21 CFR PART 11 COMPLIANCE STATEMENT

This paper explains how M-Files QMS meets or supports the requirements of U.S. 21 CFR Part 11 for both electronic records and electronic signatures.

Part 11 contains

- requirements that are about the computer system itself
- requirements that can only be met via a local procedures or personnel

We clearly mention in this paper which ones we consider to be the latter type, together with some best practices or recommendations. As 21 CFR Part 11 final rule was originally published in 1997, some of its requirements also call for interpretation or clarification based on today's IT standards.

SUBPART B--ELECTRONIC RECORDS

SEC. 11.10 CONTROLS FOR CLOSED SYSTEMS

Requirement	How we interpret the requirement	How requirement is met.
Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following: (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	User organization needs to define their user and functional requirements, test their own production implementation against those requirements, and document the results according to their own validation procedure. Special emphasis should be put to creation, modification, signing and deletion of records in the system.	M-Files QMS as a software is designed and tested to meet the technical Part 11 requirements. M-Files QMS system has been validated by our current customers, and is in GxP critical use across different life science industries and healthcare organizations. M-Files QMS system has by very core design a full time stamped audit trail plus the ability to include any necessary data validation, advanced permission settings, system checks, alerts and notifications, user organizations can ensure M-Files QMS system's ability to discern invalid or altered records. That being said, validation is not only about the qualities of the GxP related software product, but largely contains requirements that can only be met through local good practices e.g. user training, SOPs covering system use, protecting the IT environment or domain M-Files QMS system is a part of, performing recurring disaster recovery rehearsals etc. M-Files provides as an option a validation model and related services. Due to high level of configurability of M-Files QMS system, resulting in different intended use areas, we expect to discuss the details of system validation separately.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	Inspectors need to be able to search, browse and view all documents and data in M-Files. This may take place via logging directly into the system with inspector present, exporting electronic files or reports to another media for inspection purposes, or producing paper printouts.	Several options in place for meeting this requirement, according to local inspection requirements. All system documents, data and log events can be copied outside M-Files, published through another application, or exported as printable documents for inspection purposes. If an inspector would take a direct login to M-Files, it is then possible to create a listing of all documents that were opened for viewing by the inspector. Any document's or record's full version history, including all document related work, approvals, signatures, assignments, comments and metadata

		changes are immediately visible.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	System must fully record all changes to records, including record deletion. Furthermore, there must be policy in place about who can modify what, and proof that this policy is being followed.	Full version history kept. Only soft delete allowed i.e. deleted documents are still kept in the repository, and only labeled deleted. All necessary access controls can be applied to records, based on user organizations requirements. Any records' current and past permissions, or any user's access permissions, can be resolved through M-Files tools. Controls against permanent system or data loss can be achieved via backups, replications, or combination of the two both, according to user organization's requirements. M-Files QMS supports meeting desired retention, archiving or off-site long term storage of finalized content, including built-in support for PDF/A-1b archiving format.
(d) Limiting system access to authorized individuals.	User organization needs to have a process in place for controlling both users' unique user credentials, and the necessary user groups that can access M-Files repository. User organization needs to be at all times aware of who has login access to M-Files, and what kind of access each set of credentials give once user has logged on.	M-Files relies on industry standard Active Directory for both login access (authentication) and group/role based access within the boundaries of the system after successful login (authorization). This requirement is thus met, given that user organization's basic IT and access control processes are adequate and systematically followed.
(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Full history of any document, records or piece of database information must be kept. Besides changes to data itself, the history shall include all other types of activities, including workflow state changes, adding comments, changing permissions and opening the records for viewing or printing.	Requirement fully met. This is based on following: 1) each version of each document, file and database record is kept automatically, and this feature cannot be switched off by any user (including any Administrator or Super user); 2) version history also covers not only file versions but also all changes to object properties (metadata); 3) audit trail covers also non-modifying actions such as system logins and opening a document for viewing; audit trail information instantly visible both in record's own version history plus a full system log on the M-Files server. Each log item is a full report of the action, and contains who and when did the associated action. Log records are kept within the M-Files system, and can from there be either manually exported out of the system for inspection, or automatically replicated to another location in XML format. Several options available for specifying the

		desired date/timestamp format as well as system standard time zone, including UTC, as dictated by FDA guidance.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Must be able to force predefined processing workflows to selected types of documents or records. Must be able to control who is able to complete which step in those workflows.	Requirement fully met with the workflow features in M-Files. It is possible to define for each workflow state users that are able to complete the action, and to define users to whom the record is visible in different workflow states. It is possible e.g. make document visible to entire organization only when it is approved and signed. Finally, each workflow step may include any necessary data validation checks, including relational-non-trivial checks e.g. allow approving of a product batch only if all three expected test reports about the batch can be found, and have been previously passed and approved with signature.
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	User organization needs to a) establish a clear one-to-one relation between personnel and their personal login accounts (that is: ***one authorized person = exactly one named user account***) and b) establish controls for users and user groups vs. what they are authorized to see and do within M-Files system.	Part a) of the requirement is not about M-Files, but user organization's basic IT processes (e.g. access control or user management policy). Part b) is fully met: user organization can fully control login access (that is: authentication), access to documents and data within the system, and finally, control who is able to complete any given workflow action e.g. sign and approve any given type of document (that is: authorization within the system boundaries after login authentication). Current effective permissions of any document, form or database record are viewable with M-Files UI for simplified validation testing and daily use.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	It should be possible to apply necessary edit checks and data validity rules in the system.	Requirement fully met through system metadata checks and data validation rules (a.k.a. non-trivial edit checks) applied automatically to any record type when saving, modifying, or moving it to its next possible workflow state.
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.		We indeed consider lack of end-user or administrator skill perhaps the greatest single potential source or quality issues and non-compliance within the boundaries of any GxP-related IT solution. For an M-Files QMS implementation we highly recommend the following: 1. Ensure key users are formally trained and certified via ***M-Files Academy*** professional online training services, including

		certifications tests. Find out more: watch an online video or check http://m-files.com/elearning 2. Budget enough time and resources for a local training plan execution as a part of system validation. M-Files and our partners can provide tailored training services. 3. Once validated, consider using M-Files QMS' built-in training capabilities to ensure all users, including new personnel or personnel changing roles in the organization, have taken all the necessary in-house system trainings and hold a valid training records at all times. Use M-Files QMS to force mandatory refresher trainings according to desired schedule. 4. During QMS production use consider using M-Files QMS' document learning capabilities to turn any QMS system-related key documents (SOPS, instructions, QMS user guide, etc.) into trainable documents with eSignature controlled learned-and-understood process and mandatory re-learning. Both M-Files professional training services as well as M-Files QMS system's own built-in learning capabilities are relevant but big topics, so we're happy to discuss them separately.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.		This requirement is not about M-Files system, but calls for a local procedure. It is highly recommended to not only have the full SOP life cycle in M-Files QMS, but to also exploit its built-in document learning capabilities. User organizations can thus make sure that each personnel is aware of the procedures that apply to them. Training records for written policies can be obtained via self-signed Read & Understood method, or via train-by-trainer approach. We're happy to discuss the details this very relevant but vast topic separately.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system		All necessary system documentation, training material, training records, system specific SOPs and user manuals can be fully controlled within the system itself, published via another system, or training copy document binders, according to user organization's own policy.

operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.		

SEC. 11.30 CONTROLS FOR OPEN SYSTEMS

According to 21 CFR Part 11 an open system is defined as: ***an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.***

In any typical M-Files QMS implementation the organization using the system is solely responsible for its contents, and also controls the system access from legal as well as technical point of view. This statement holds also for M-Files Cloud Vault as login accounts and system access is controlled by the user organization. Naturally within an organization there may be groups of people more responsible for certain Part 11 related content, while organization's IT department controls system access from a technical point of view. But even in such a case the organization as a whole both controls access and is responsible for the content. Finally, we would never recommend having IT department or other purely technical personnel alone control and authorize access to a Part 11 compliant, validated system. Instead there should be a process in place where access is formally requested, authorized by responsible managers or system owners, and technically executed by IT department. With such a process system access is truly authorized by persons responsible for the content of electronic records that are on the system. We therefore conclude that ***M-Files QMS is a closed system***, and requirements related to open systems do not apply.

As a further discussion we would like to add that it is possible as such to create an open M-Files system through customization. This could be done for example by providing a public website where any user can self-register and choose a login identity and password. Another example would be providing M-Files client terminals in public spaces with no login authentication whatsoever, thus providing system access to any person who physically has access to such terminal or client device. As the reader can see, use cases like this are quite far-fetched and theoretical, and never recommended by M-Files Corporation for Part 11 compliant system. We hope this example further clarifies why we indeed consider M-Files QMS a closed system.

SEC. 11.50 SIGNATURE MANIFESTATIONS

Requirement	How we interpret the requirement	M-Files response
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	All the required information on the left should be instantly visible both in the system itself and, in the case of electronic documents viewable in their native programs (such as PDF viewer or MS Office programs), the signature information should be automatically rendered on the document itself, either to document header/footer/watermark or separate signature information page.	M-Files QMS fully meets the requirement. All associated logging is automatic and mandatory by the system design. Time-stamped logging about the signing steps are visible both through the signed record and through system wide audit trail log. In case of traditional printable PDF documents signed in the M-Files QMS, the system allows any necessary document rendering and server-side manipulation to both provide the necessary signed document appearance and/or provide any necessary information about the signatures, signers and timestamps on the printable document itself.
(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record(such as electronic display or printout).	There needs to be a full time stamped audit trail log for each signing event, and, each document's or record's own version history should instantly reveal who and when have applied what signatures on the document.	M-Files fully meets the requirement, and all associated logging is mandatory by the system design. How the information of the signature(s) is rendered to the documents is defined for each document template separately, with options including document header or footer on every page, a watermark sampling across all pages, the document title, and a separate, computer-generated signature page.

SEC. 11.70 SIGNATURE/RECORD LINKING

Requirement	How we interpret the requirement	M-Files response
Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary	System must only allow record signing via a predefined, controlled workflow. Copying any text or image on top of any document, or modifying its metadata properties to contain any signing-type information, must never be equal to having the document in its finalized and	M-Files fully meets the requirement. Necessary controls are in place to control who can apply which type of signature to which type of record. The link between the record and its signature cannot be broken. In some cases an existing eSignature may be invalidated due to a consecutive approver's rejection of approval. In

means.	signed state.	such cases document's version history and system audit reveals also invalidated signatures.

SUBPART C--ELECTRONIC SIGNATURES

SEC. 11.100 GENERAL REQUIREMENTS

Requirement	How we interpret the requirement	M-Files response
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each eSigning token or credentials are linked to exactly one real person. There are controls against using other person's credentials.	The Part 11 electronic signing in M-Files QMS is based on the use of Windows credentials, which ensures that each signing credential is unique. Thus requirement is fully met, given that user organization has necessary access control measures in place i.e. how personnel are given their unique user credentials, and how necessary signing complexity is ensured via standard domain settings. User organization may apply available strong authentication methods when either logging into M-Files or signing electronically. M-Files QMS can through implementation work comply with selected two-factor ***strong authentication*** methods for additional signing security. We wish to discuss the details separately as per user organization's requirements. Finally, M-Files QMS has built-in support for certificate-based ***digital signing,*** providing additional level of security beyond the more common electronic signing. Digital signatures provide means to protect documents' integrity and authenticity also in cases where documents are exported or published form M-Files QMS system, and/or sent out or submitted from their originating organization. Digital signature is currently limited to PDF file format and file formats than M-Files can convert into PDF, including but not limited to MS Office documents. Digital signing is not currently mandated by FDA, but we see it becoming the common best practice for regulated life sciences. We're happy to discuss the details separately. For more info see e.g. : http://en.wikipedia.org/wiki/Digital_signature

Requirement	How we interpret the requirement	M-Files response
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.		This requirement is not about M-Files software.
(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures. (1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. (2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.		This requirement is not about M-Files software.

SEC. 11.200 ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

Requirement	How we interpret the requirement	M-Files response

Requirement	How we interpret the requirement	M-Files response
(a) Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	Must have at minimum personal username (clearly distinguishable Common Name recommended) and password with necessary complexity, as enforced by the account password policies in Windows.	M-Files users are authenticated against Windows credentials. User organization's access control policies should be enforced both through written SOPs as well as technical controls provided by Windows. M-Files QMS can through implementation work comply with selected two-factor ***strong authentication*** methods for additional signing security. We wish to discuss the details separately as per user organization's requirements.
(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.		Electronic signing only possible one record at the time, always utilizing all signature components. M-Files allows setting up surrogate signing and batch signing workflows. For example, signing of a training event will also apply instructor's signature on each training certificate created for each trainee. In surrogate and batch signing scenarios each signature will by very design contain every single signature component. Such setups should receive special attention in system validation.
(2) Be used only by their genuine owners	User organization needs to establish strong relation between each person and his/hers user credentials, and have controls against using other person's credentials deliberately or by accident.	This requirement is not about M-Files system.
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more		Requirement met, given that basic IT administration and M-Files administration is federated among two admin user groups, or other controls put in place for replicating essential system access data to an independent third party, not

Requirement	How we interpret the requirement	M-Files response
individuals.		accessible by local IT administration.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.		Biometrics authentication or eSigning may be utilized for authenticating against Windows Active Directory domain. Thus this requirement is not about M-Files software.

SEC. 11.300 CONTROLS FOR IDENTIFICATION CODES/PASSWORDS

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

Requirement	How we interpret the requirement	M-Files response
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.		This requirement not about M-Files system. Typically this requirement is met via user organization's own basic IT processes e.g. centralizing all user credentials to an industry standard single-sign-on domain that ensures uniqueness.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).		This requirement not about M-Files system. Typically this requirement is met via user organization's own access control policy, often using Active Directory Domain's Group Policy Objects
(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.		This requirement not about M-Files system. Typically this requirement is met via user organization's own access control policy or IT maintenance processes.
(d) Use of transaction safeguards to prevent unauthorized use of passwords		This requirement not about M-Files system. Typically this requirement is met via user

Requirement	How we interpret the requirement	M-Files response
and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.		organization's own access control policy. We're happy to discuss separately user organization's special requirements for additional safeguards for password or identification, e.g. in the form of strong authentication methods.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.		This requirement not about M-Files system. Typically this requirement is met via user organization's own access control policy. M-Files QMS can be used as a helpful tool to provide reminders of any periodic testing activities and recording of their results. This is done with built-in Periodic Task method i.e. same method used for e.g. periodic review of effective quality documents.