SOLABS QM10: Security and Incident Management

Table of Contents

Purpose of this Guide

This guide is intended for SOLABS QM10 System Owners who perform advanced setup, maintenance and administration activities in **SOLABS QM10**. It provides information on how Security and Incident Management is handled for SOLABS QM10 and can be used as a template for creation of a local Security and Incident Management document.

System Description

SOLABS QM10 is a fully integrated Enterprise Quality Management System (EQMS) software solution developed specifically for Life Sciences companies. SOLABS QM10 is a Web-based system deployed on a server-side setup. A Web-browser provides the interface to the system users, so no software needs to be installed on the users' workstations. SOLABS QM10 is mostly a server-end system. The system creates and maintains GxP-regulated electronic records and thus requires compliance with U.S. FDA regulations 21 CFR Part 11, Electronic Records, Electronic Signatures. The records (documents, training records, change control process steps, etc.) generated in the system remain in it for the whole life cycle.

The SOLABS QM10 system is composed of the Core software – QM Essentials - for the management of documentation and auditing with additional capability to deploy training management and quality processes such as Change Control, Deviations, Complaints, etc.

General System Configuration

System Setup

SOLABS QM10 is a web-based application accessed through a URL. Usernames and passwords are unique for each user.

System Requirements

SOLABS QM10 is an internet-based application which requires the following end-user components and settings:

- Web Browser – (define as per client)
- Other – (define as per client)

System Parameters

The following system parameters are set as defaults in SOLABS QM10 and can be adjusted during initial configuration of the client environment:

- Session time out delay is 15 minutes.
- Password requirements for hosted Production environments are established in Password Management and applied as Users create their passwords (unless an available SSO option such as Microsoft Azure, Onelogin or Okta are chosen deployed).
- Accounts are locked after 5 invalid login/e-Signature attempts.

Electronic Signature

Electronic signature (dual authentication) is required for the following activities:

- Confirming a Training Assignment
- Approving a Document
- Signing off on a Process Step

Audit Trail

SOLABS QM10 includes a pre-configured audit trail on Users, Documents, Training Activities and Processes. The audit trail is accessible to users with the appropriate level of privileges.

System Access

The **SETUP** section is used to manage **System Access** and **System Parameters**. It is available to Users who have been assigned the System Role of **SOLABS System Administrator**.

Definitions

- System Owner: The system owner is the individual responsible for the implementation, operation, maintenance, and retirement of an information system.
- SOLABS System Administrator: Individual(s) identified by the Management deemed as having the appropriate level of expertise to successfully administer the software and is therefore assigned the applicable System Administration Roles in SOLABS QM10 (SOLABS System Administrator, SOLABS Document Administrator, SOLABS Training Administrator, SOLABS Help Desk).
- User: A user account, here called User, is a mechanism by which the software identifies different persons who use the software.
- Role: A role is a named grouping of that can be assigned to users in SOLABS QM10. Roles can be used to manage document privileges, assign training and manage access to process workflow steps.
- Incident: Any event which is not part of the standard operation of SOLABs QM10 and which causes, or may cause, an interruption to, or a reduction in, the quality of the related functionality. Incident also includes standard service requests.

Typical Responsibilities

Function	Responsibilities
SOLABS System Owner & Administrator	Ensure the computerized system is configured, validated, used, and maintained in a manner consistent with written policies, procedures, and regulations. • Manage system upgrades/fixes • Manage change control • Define procedures • Set System support and incident management. Has a full knowledge of the Set-up section, and is assigned the System and Document Administrator roles in SOLABS QM10 in order to: • Maintain the Security Roles in accordance with the organizational chart • Manage the configuration of the system (Roles, Users, Document Types, Document Workflow Templates, PDF Rendering Templates, System Configuration, System Attributes and Custom Lists) • Manage privileges on folders and documents
IT	• Provide resources for the computerized systems validation and maintenance. • Ensure the network infrastructure is consistent with policies, procedures, and regulatory expectations. • Support system owner with incident management. • Unlock users.
Document Coordinator	Has a full knowledge of the Document section, and is assigned the SOLABS Document Administrator role in SOLABS QM10: • Process Document Control Requests from request until document approval. • Manage folder structure.
Training Coordinator	Has a full knowledge of the Training section in SOLABS QM10 and is assigned the SOLABS Training Administrator role in SOLABS QM10: • Manage training curriculum and training activities. • Assign training.
Department Head	• Request user access or deactivation for SOLABS QM10 system.
User	• Use the system. • Inform a SOLABS Administrator of any issue with the software.

User Management

There are three types of **Users** available in **SOLABS QM10**. These are defined as **Account Types** when setting up the User and are associated with the following levels of access within the system.

- **Standard**: This Account Type is required for anyone who will perform transactions in the system, from Document Review/Approval to Task Completion, to Acting on a Process Workflow Task to Administration of the System.
- **Train ID**: This Account Type provides only view access to documents for training purposes. It is useful when you have users who will need no other access to the system or when you need to limit access for any reason.
- **External:** This Account Type can be used for contractors, auditors, or others outside the company, who may need access to view information and/or be involved in other assigned **SOLABS QM10** related interactions such as document review/approval. **NOTE:** They are not given access to **Search** and any **Views** are limited to outstanding activities assigned to them.

Role Management

There are four types of **Roles** available in **SOLABS QM10.** Users can be assigned one or more as required. Role Management actions require assignment of the System Role **SOLABS System Administrator**.

Role Type	Description
Security Role	Assigned to defines what part(s) of the organization a user belongs to: • Department, • Sub-Department • Division • Organization Security Roles can be used to set Document privileges and are helpful in running Reports.
Function Role	Assigned to define the User's Job Title and/or other Function Role(s). Function Roles can be used to define and assign required Training Activities and to establish meaning of signature for document review/approval tasks and process tasks.
Process Role	Associated with **SOLABS QM Process APPs** and assigned to define a User's responsibility in a given process workflow. These roles are deployed with the Process APP at installation and qualification and cannot be modified.
System Role	Reserved for specific individuals involved in **SOLABS System Administration** activities. • SOLABS System Administrator – can manage Users, Roles and System Configurations. • SOLABS Document Administrator – can manage Custom Lists, System Attributes, Document types, Document Workflow Templates and PDF Rendering Templates. • SOLABS Training Administrator – can create Curriculum and Training Activities, can manage training assignments. • SOLABS Help Desk – can unlock users and reset passwords.

Managing Privileges in the Document Section

The **Privileges** settings define the type of access the Users have to the different folders and/or documents. This access is granted by Roles. When those Roles are assigned to a User, they then have the related Privileges.

By default, Users with the System Roles of SOLABS Document Administrator and SOLABS System Administrator have Full Control. Users with only the SOLABS General User role – Train ID Users for example – have the lowest Privilege of Read Only.

Privilege Levels in the Document Section:

- **Read Only** = Users with this privilege can view Approved & Effective documents or Approved, Not Effective documents assigned to them for training purposes.
- **Review/Approve** = Users can do the above as well as act on document Review or Approval tasks.
- **Modify** = Users with this privilege can do the above and can also create and modify documents.
- **Administer** = Users with this privilege can do all of the above and can also set privileges.

Managing Privileges in the PROCESS Section

For any of the SOLABS QM Process APPs, the major steps in the process are displayed in the Process Flowchart by dark-shaded boxes. These major steps are considered Primary Tasks in the process.

Decisions made by those involved in the process act to progress it to the next Step or return it to a prior Step. There are Process Roles that need to be assigned to the Users in SOLABS QM10 who will make the related decisions. If these Process Roles are not assigned to any Users, the Process workflow will not move forward or will instead be assigned to users with SOLABS System Administrator or SOLABS Document Administrator roles.

Process Roles are available with the deployment of a Process APP and can be assigned to Users by the SOLABS System Administrator.

Privilege Levels in the Process Section are described in the following table.

	Act On	Act On & Reassign	Modify	Administer
Start Process	X	X	X	X
View	X	X	X	X
Act On	X	X	X	X
Email Link	X	X	X	X
Get Link	X	X	X	X
Link Documents to OPEN Processes	X	X	X	X
Link Processes to OPEN Processes	X	X	X	X
Modify Description on OPEN Processes	X	X	X	X
Remove Links on OPEN Processes	X	X	X	X
Summary Report				

View Audit Trail		X	X	X
Move Out of Waiting		X	X	X
Reassign tasks currently assigned to me		X	X	X
Link Documents to CLOSED Processes			X	X
Link Processes to CLOSED Processes			X	X
Modify Description on CLOSED Processes			X	X
Modify Values on OPEN process			X	X
Reassign all process tasks			X	X
Cancel				X
Manage Privileges				X
Modify values on CLOSED process				X

Maintenance of the SOLABS QM10 System Validated State

The system validation and testing are performed according to the *SOLABS QM10 Validation Plan*. The following are considered as milestones that need to be achieved and/or practices that need to be embraced to obtain and maintain a validated state for the SOLABS QM10 system.

System Ongoing Monitoring

Ongoing monitoring of the incidents with the system is performed to assure that the whole system is under control during the "live" phase of the project. It is intended to ensure the quality and integrity of the data at the different steps of the data life cycle. Any issue that could have an impact on the quality or integrity of the data will be addressed and escalated as defined by applicable quality management SOPs.

Change Control

Any change made to SOLABS QM10 system once validated can compromise the validated state of the system. The company change control procedure will be followed to ensure that any proposed change to the system is evaluated for the impact on the validated state of the system and to determine re-validation activities (if any). If the original validated state will be impacted as a result of the change, re-validation activities are performed as described in the associated change request.

Any modification to the validated system should be approved by the SOLABS System Owner and a QA representative prior to its implementation into the production environment.

Periodic Review

A periodic review of the SOLABS QM10 system should be done every year to verify that it remains compliant with regulatory requirements, fit for intended use and satisfies company policies and procedures. The following items should be part of the annual review:

- Operation and maintenance documentation (CAPA and/or CC)

- System incident log
- Configuration Documents
- Any change in use of the system
- Outstanding actions from a validation report
- Outstanding actions from a previous review or audit
- System Security and Access Control (review of user access and training)
- Software and data backups are still in place and function effectively.

Data Security and System Availability

Use this section to describe security depending on whether system is installed locally or hosted. Local installations would include physical access and controls. Information for hosted installations can be provided by SOLABS.

SOLABS QM10 is installed locally/hosted remotely… System security is managed as follows…

Security

Availability

Incident Management

The SOLABS QM10 system has a lot of functionality and it is anticipated that software issues could potentially arise during use. Those incidents could prevent the users from using the software to complete their task or could affect the proper working of the software as described in the User and Functional Requirements. It is the responsibility of the users to inform a SOLABS Administrator of any issue with the software.

The following sections are provided as examples *but should be filled in according to company policies/procedures.*

SOLABS Support Desk

For technical questions contact the local SOLABS System Administrator.

Incidents Classification

SOLABS system incidents are classified in 3 categories based on their severity:

- Level 1: Low-priority incidents; mainly standard service requests. It does not interrupt the business and can be worked around.
- Level 2: Medium-priority incidents affect a few users and interrupt work to some degree. May necessitate actions by IT or software vendor.
- Level 3: High-priority incidents affect a large number of users and interrupt business processes. Necessitate actions by IT or software vendor.

The following table provide examples of incident classification:

Incident Category	Example of incidents	Type of incident	Responsible	Record in Incident log?
Level 1	Account locked	Standard service requests	SOLABS Help Desk	No
Level 1	Cannot access documents or participate in a review cycle – privileges issue	Standard service requests	SOLABS Administrator	No [i)]
Level 1	User cannot perform actions - training issues	Standard service requests	SOLABS Administrator	No
Level 2	Malfunction that affects few users and interrupt work to some degree for example: – Search function not working – Document not converted to PDF – Cannot confirm a training	Malfunction	System Owner	Yes
Level 3	Malfunction that affects a large number of users and interrupts work for example: – System not responding – Process not working (DOC, CC, etc.) – Cannot access any documents	Critical Malfunction	System Owner	Yes

Incidents Log

Level 2 and 3 incidents must be logged in the system incident log. The log should include, but is not limited to:

- Incident ID (year followed by chronological number, e.g., SOLABS-2017-001)
- Vendor ticket ID, if applicable
- Change Control ID, if applicable
- Incident Category
- Initiation Date
- Completion Date
- Description of issue (including cause and resolution as applicable)
- Status (Open/Closed)

An appropriate follow-up must be performed for any system incident. If deemed required, a CAPA might be initiated to investigate the issue and determined if corrective actions are required.