

21 CFR Part 11 Compliance Assessment

Compliance Software Solutions Corporation (CSSC) has developed the Microbiology Information Management System (MIMS[®]), Version 1.0x to comply with the requirements defined in the FDA's 21 CFR Part 11 for Electronic Documents. The MIMS is a closed system designed to ensure accuracy, reliability, and consistently intended performance. As established in the regulation, MIMS incorporates the following:

Requirement	MIMS Assessment
Validation	CSSC offers a release testing package for the program. It includes documentation of the implementation and coding, traceability analysis, integration testing, installation testing, and boundary testing.
Audit Trails	The independent and non-modifiable Audit function provides for secure, computer-generated date and time stamp of record changes and key operator entries and activities. Actions that insert, update, or delete records are retained for viewing and / or printing. Reports can be generated by date range and table (audit record).
System Security	<p>System access is limited to authorized and qualified users as established in the Security database. Security access and the permissions / access granted to those security levels are established in the MIMS by the System Administrator. Users can be granted permission to access only specific applications / functions within the MIMS, as well as granted permission to access only certain defined buildings or areas that are established within the locations database. The system Administrator has the option of establishing as many levels of security as is necessary.</p> <p>The MIMS has a log out security feature, which is automatically activated once the pre-set period of time (1 – 30 minutes in one minute increments) has been met. This ensures that should a workstation be left unattended, an unauthorized individual cannot access the application.</p>

Requirement	MIMS Assessment
Password Maintenance	<p>The MIMS provides for initial and periodic testing, as well as a user defined password expiration interval. Password expiration dates are defined and set by the System Administrator (from 1 – 90 days in 1 day increments). Only the System Administrator has access to modify the security settings.</p> <p>Once a password expires, consecutive passwords cannot be the same. Passwords can be alpha numeric, and must be 6 to 15 characters. As an option, the System Administrator can <u>require</u> that passwords be complex (i.e. both alpha and numeric characters).</p>
Record Retention, Protection, Retrievability, and Reproducibility	<p>The MIMS has been designed and tested to accurately retrieve and generate all reports and database records. All electronically stored records are validated to be able to be accurately generated, retained, protected, and readily retrieved in both “human readable and electronic form” throughout the retention period. A validated archive and unarchive feature further adds to the record retention and reporting capability.</p>
Operational Checks	<p>Where necessary, the appropriate operational checks have been put in place to enforce step and event sequencing. The program will only allow events to be performed in the appropriate sequence. It is not possible to perform certain steps before others are complete.</p>
Authority Checks	<p>Only authorized personnel have access to the application, and the ability to use the system. Security access is set by the System Administrator. Each level of security established by the System Administrator has unique, restricted access to the program’s functions and locations.</p> <p>The MIMS has built-in security protection that does not allow a user to make more than three attempts to log into the system. After the third unsuccessful attempt to login, the user is “locked out” of the MIMS and only the System Administrator can “unlock” the user. When a user is locked out of the system, an e-mail can be sent to a designated individual(s) notifying them of the lock-out.</p>
Device Checks	<p>Only terminals with the MIMS installed can make data modifications / entries. This ensures the validity of the source of the data input and / or operational instruction.</p>

Requirement	MIMS Assessment
Documentation Controls	A single copy of all system documentation is provided with the site license.
Electronic Signature Security	Only those users established in the security database that have been granted access to the MIMS can login. Attempting to enter an incorrect password three times will lock the user out of the program. Only the System Administrator will then be able to unlock that user ID.
Password Security	Controls ensure the security, integrity, and uniqueness of the identification and password combination used for login and electronic signature. Passwords must be between 6 and 15 characters. User ID and Password combinations are unique. Passwords are encrypted when entered in the application, as well as when they are viewed in the database.
Electronic Signature Assignment	Each user's unique electronic signature cannot be reused or reassigned to another user. Each user name and password combination is unique. Once a password expires it cannot be reused consecutively.
Electronic Signatures Not Based Upon Biometrics	<p>Both a user name and password are required for initial login. Both are required on subsequent logins when security logoff has occurred due to inactivity in the MIMS.</p> <p>In order to perform inserts, updates, or deletions to any records, the authorized user is required to authenticate their identity by signing into the function and re-entering his or her user name and / or password. An optional setting for electronic signatures can require both a user name <u>and</u> password be entered to sign a record, or just a password. In the latter instance, the signing will default the user name to the person logged into the MIMS. The activity performed is then captured in the audit, and a full manifestation of that individual's name will appear in the audit record.</p>
Electronic Signature With Biometric Links	The system is designed to preclude use by anyone except a genuine user. If an individual is not established in the Security database there is no ability to access any function within the MIMS.

Requirement	MIMS Assessment
Name Display	The printed name of the individual who signs a record electronically is always clearly displayed. His or her user name will appear on relevant documents and reports generated by the program. The user ID of the individual logged into the MIMS is prominently displayed on the title task bar of the program window.
Signature Purpose	The meaning of each electronic signature, as defined by the individual organization, must be coupled with the appropriate procedures and training.
Signature Binding	Electronic signatures cannot be cut, or copied and pasted, or transferred by any means. When required, those names established in the Security database can be entered in fields by means of the drop down menu.