21 CFR Part 11 Compliance – Checklist

Paragraph	Short description	Implementation in Intellilog Manager	Status
11.10	Controls for closed systems	Intellilog Manager is designed to be a closed system and uses username and password credentials to authenticate each user.	✔
11.10a	Validation of systems	Argo Ubicom GmbH has verified and validated Intellilog Manager according to GAMP5. Through audit trails for user and quality relevant data changes to your data are always tracked. We also provide relevant software documentation for inspection.	✔
11.10b	FDA copies	All quality relevant data is available electronically as well as in a human readable format.	✔
11.10c	Protection and recoverability	Intellilog Manager is running on at least two distributed servers in parallel. This ensures high availability and duplication of the data (fail-over). Furthermore, we regularly backup the data for added protection. Intellilog Manager also provides export functionality in the longtime archiving ISO 19005 format (PDF/A), which can be integrated in the customers backup process. The protection of the data is therefore given from its creation until archiving and government archiving rules can be met.	✔
11.10d	Limiting system access to authorized individuals.	Access to the data is given only to authorized persons with individual usernames and passwords. Password aging and access locking after multiple wrong attempts are just a few of Intellilog Managers security functionalities.	✔
11.10e	Audit trails	All quality relevant data have an audit trail. This audit trail tracks changes user specific and exact to the second. These unmodifiable audit trails are available electronically as well as in human readable form. The audit trails are, as the underlying data, backed up and available in the long-time archiving format PDF/A.	✔
11.10f	Operation sequences	Whenever actions must be performed in a specific sequence the system enforces this sequence and therefore prevents accidental changes to data.	✔
11.10g	Authority checks	Intellilog Manager has an elaborate role-based authority concept which meets the requirements of 21 CFR Part 11.	✔
11.10h	Device checks	The system has validated input and output interfaces. The webservice based interfaces accept and provide data securely in the so called JSON format.	✔
11.10i	Training	All experts which are involved in the create and maintenance of Intellilog Manager are trained in computer system validation and 21 CFR Part 11 compliance. Furthermore, special training and documentation as standard operation procedures are given to back-office personnel to ensure that they have the skills to perform the assigned tasks.	✔
11.10j	Establishment and adherence	Apart from the points mentioned in 11.10i, we are happy to help you with the creation and implementation of policies and employee training.	✔

	to written policies		
11.10k	Control over documentation	Our software documentation is validated through a strict review and versioning process. Furthermore, we ensure that each user has a user manual specific to his role.	✓
11.30	Controls for open systems	This point does not apply since Intellilog Manager is designed to be a closed system.	✓
11.50a/b	Signature manifestations	This point does not apply since Intellilog Manager does not make use of electronic/digital signatures.	✓
11.70	Signature/record linking	This point does not apply since Intellilog Manager does not make use of electronic/digital signatures.	✓
11.100a, b, c	Electronic signatures	This point does not apply since Intellilog Manager does not make use of electronic/digital signatures.	✓
11.200a, b	Electronic signature components	This point does not apply since Intellilog Manager does not make use of electronic/digital signatures.	✓
11.300a	Uniqueness of each combined identification code and password	The system ensures that the login credentials are always unique.	✓
11.300b	Changing and aging of credentials	The system enforces passwords to be changed after a certain period. Furthermore, authorized personnel can lock and unlock certain users if necessary.	✓
11.300c	Loss management procedures	This point does not apply since Intellilog Manager does not make use of any hardware to identify individual. The username/password credentials are the only way to get access to the system.	✓
11.300d	Safeguards to prevent unauthorized access	Users are locked out from the system if their passwords were entered wrongly multiple times in a row. Unlocking users is only possible through authorized users. Furthermore, each locking and unlocking event is tracked in an audit trail.	✓
11.300e	Initial and periodic testing of authentication devices	This point does not apply since Intellilog Manager does not make use of any hardware to identify individual. The username/password credentials are the only way to get access to the system.	✓

✓ Fulfilled   ✓ Not relevant   ✗ Not fulfilled

✓

Intellilog Manager is 21 CFR Part 11 compliant