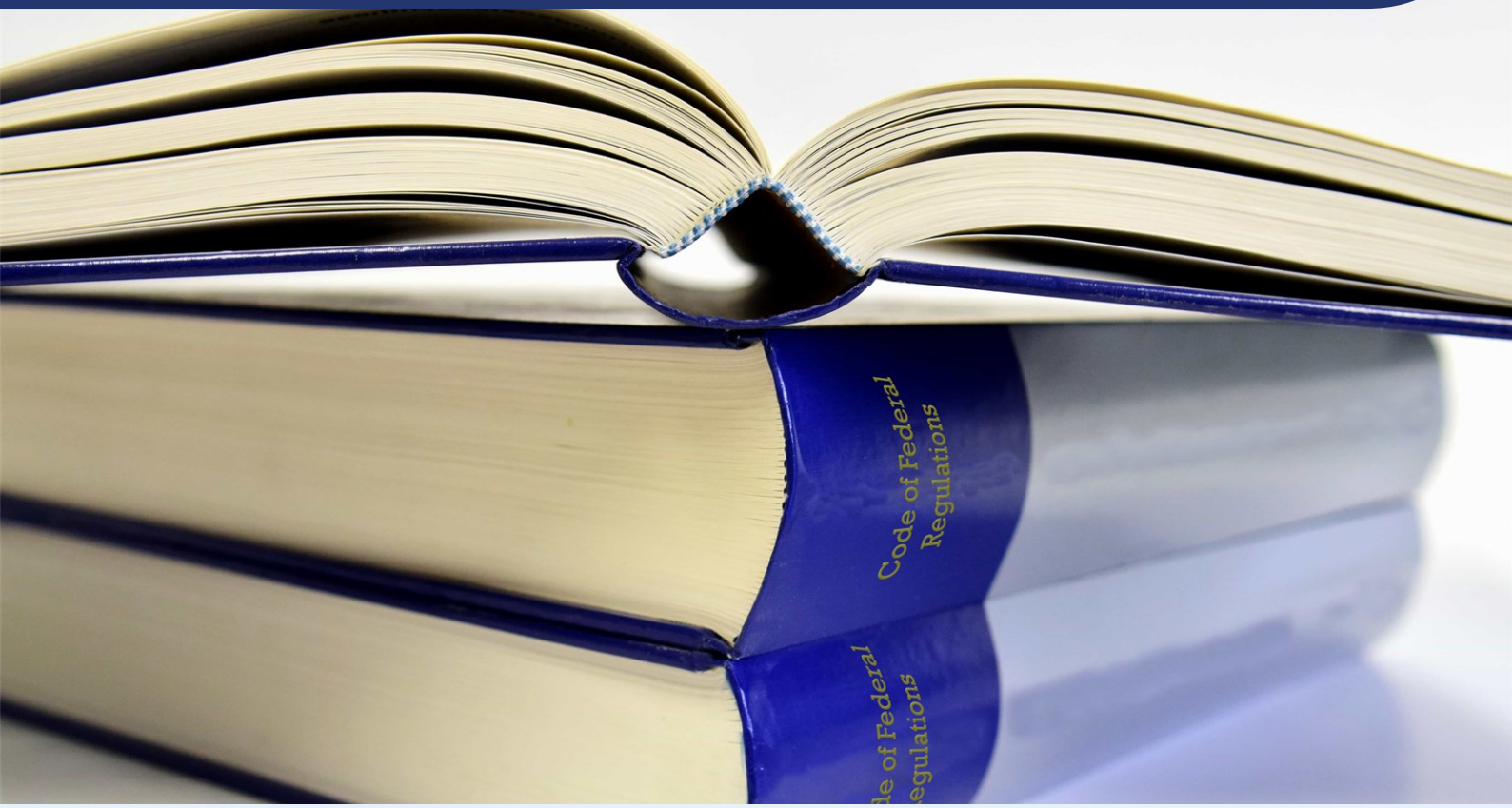

LogTag Digital Signatures

Compliance Document

FDA Title 21 Part 11 Electronic Records, Electronic Signatures

Software Revision 3.2

Document Revision 2

Published July 15, 2022

Introduction

The FDA sets out requirements for electronic records and electronic signatures in its Code of Federal Regulations Title 21--FOOD AND DRUGS, CHAPTER I--FOOD AND DRUG ADMINISTRATION, DEPARTMENT OF HEALTH AND HUMAN SERVICES, SUBCHAPTER A--GENERAL, PART 11 -- ELECTRONIC RECORDS; ELECTRONIC SIGNATURES, also commonly known as FDA 21 CFR Part 11.

Ten paragraphs in three sections (also called subparts) of the regulations can be summarized as follows:

- General Provisions

  This subpart outlines the scope of the regulations, the requirements of its implementation and which terms and definitions the document uses.

- Electronic Records

  This subpart lists requirements for controlling closed and open electronic systems, how signatures are manifested and how they are linked to records.

- Electronic Signatures

  This subpart details general requirements for electronic signatures, which components and controls should be implemented and how they are controlled and identified.

The following pages detail how LogTag® Analyzer fulfils these requirements. The code's text is cited, along with an explanation how the software addresses and complies with the requirements.

The Electronic Records and Electronic Signatures sections also contain information on how LogTag North America validates these requirements.

Copyright

no association with any real company, organization, email address or person is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

No representation or warranty is given and no liability is assumed by LogTag North America with respect to the accuracy or use of such information or infringement of patents or other intellectual property rights arising from such use or otherwise.

Disclaimer

LogTag® products assist with monitoring temperature and humidity exposure, but do not monitor the quality of the goods they accompany. Their purpose is to signal if product quality evaluation or further testing is required.

System Requirements

LogTag® Analyzer is compliant with the requirements published by the US Food & Drug Administration FDA 21 Title 11; Electronic Records and Electronic Signatures when used as part of the LogTag® Digital Signature Suite, which can be accessed from the LogTag North America website at https://logtagrecorders.com/software/dss/.

The document assumes the use of:

- LogTag® User Server, version 1.3 or later
- LogTag® Event Viewer, version 1.1 or later
- LogTag® Analyzer, version 3.2r1 or later

Please refer to the User Guides of these programs for detailed instructions and system prerequisites. Additional information can be found in the LogTag® Analyzer Network Guide.

Subpart A - General Provisions

§11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with §11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by §§1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(g) This part does not apply to electronic signatures obtained under §101.11(d) of this chapter.

(h) This part does not apply to electronic signatures obtained under §101.8(d) of this chapter.

(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

§11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action (s) where those features and/or actions are both unique to that individual and measurable.

(4) Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) Open system means 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.

Subpart B - Electronic Records

§11.10 - Controls for closed systems

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:

Requirement	How LogTag® achieves compliance	How we test	Complies
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Each file contains several identification tags and checks, indicating if the information inside is genuine, and whether or not the data has been altered. Files that have been tampered with or are not genuine data cannot be successfully accessed.	Generate a file via download, open file with a text editor and randomly change some characters. Save the file. Read the file back into LogTag® Analyzer. Corrupted message appears.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	All files can be displayed electronically and/or printed. Users external to the system, with the appropriate software and access to the relevant files, can also electronically display and/or print the information within a file.	Generate PDF from downloaded logger, Open on PC without LogTag® Analyzer installed. Verify that embedded *.ltd file contains exact copy of PDF displayed information	✓
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	It is the responsibility of the organization to develop appropriate controls and SOP's to ensure records are available during the required retention period.	Automatic file storage can be individualized to the organization's requirements.	N/A
(d) Limiting system access to authorized individuals.	To access the system a user must provide a valid username and password. The system will only allow a user to perform the tasks that they have been granted permission to perform.	Link LogTag® Analyzer to User Server. Try to open file without logging in. Permission will be denied. Log into LogTag® Analyzer with valid credentials. Permission should be granted to open file.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	Each action involving modification and/or access to user accounts, electronic data and electronic signatures is included in an audit log file. Each action has the date/time of the event, information about the user that caused the action and the location of the user (workstation name). Actions within an audit log file can be electronically displayed and/or printed through the Event Viewer software.	Log into LogTag® Analyzer connected to User Server. Download a logger. Open Event Viewer software and locate log entries for log in attempt and file download.	✓
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Each user must perform a predefined sequence of steps, as defined by the software, to ensure each task is performed correctly.	Logger configuration and download follow prescribed processes from the software's user guide.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	Each user must provide a valid username and password to access the system. The system checks that the username and password are valid and that the user has the appropriate permission to perform the relevant task each time the user performs a task.	Link LogTag® Analyzer to User Server and log in with restricted account that cannot sign files. Download logger. Try to apply signature, action is not allowed. Now sign out and sign in with unrestricted account. Signature can now be applied.	✓
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Communication between logger and software contains several layers of checksums and identification tags to ensure the data obtained fromloggers is genuine and to determine if the data has been tampered with.	Invalidate logger checksum for calibration area inside a file. Logger cannot be downloaded. Re-validate logger checksum. Logger can now be downloaded	✓
(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.	It is the responsibility of the organization to develop appropriate resources and adequate education and training to use the system.	LogTag North America provides comprehensive User Guides for the Digital Signature Suite, the LogTag® Analyzer software and for each logger model.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	Users must agree to a statement that makes them personally liable if they try to change the system, which may allow them to falsify information and electronic signatures. It is possible to restrict a users ability within the system to change these settings, thereby reducing the possibility of the false electronic information been generated. It is otherwise the responsibility of the organization and their relevant SOP's to prevent and/or record and signature falsification.	Permission model can be individualized to the organization's requirements.	N/A
(k) Use of appropriate controls over systems documentation including:			
1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Documentation outlining implementation of the system is available. Compliance is subject to organization SOP's and their implementation of this system.	Integrated help file is tested for completeness.	✓
2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Each revision of the software that is a part of the system is unique. Changes between each revision are documented with date/time information. Each revision is tested to ensure the system functions according to specification and compliance.	Test plan covers revision numbering and release note issuing.	✓

§11.30 - Controls for open systems

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Requirement	How LogTag® achieves compliance	How we test	Complies
–	This system does not operate in an open system environment.	N/A	N/A

§11.50 - Signature manifestations

Requirement	How LogTag® achieves compliance	How we test	Comply
(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;	Each electronic signature recorded includes all user account details. As a minimum, they including the user's username (used to access the system) and full name, but may also contain description and e-mail address, where these details have been provided by the system administrator.	Sign a downloaded file, verify that the Digital Signature dialogue contains the required information.	✓

Requirement	How LogTag® achieves compliance	How we test	Comply
2. The date and time when the signature was executed; and	The date and time according to workstations the user is using to perform the electronic signature is stored, along with the the UTC time zone for when various electronic signatures are performed across time zones.	Sign a downloaded file, verify that the Digital Signature dialogue contains the required information.	✓
3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The user must choose a meaning for each electronic signature to be performed, before it can be stored. Meanings that the user can associate with the signature are defined and controlled through the User Server software, and not all users will necessarily have the same meanings to choose from. Users can only associate meanings with a signature that the User Server software has permitted.	Sign a downloaded file, verify that the Digital Signature dialogue contains the required information.	✓
(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).	Full details of electronic signatures can be viewed electronically with LogTag® Analyzer, with or without access to the User Server. The time and meaning of a signature can also be viewed from a PDF generated from a signed file.	Check the signature of a file from an installation of LogTag® Analyzer not connected to User Server.	✓

§11.70 - Signature/record linking

Requirement	How LogTag® achieves compliance	How we test	Comply
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 means.	Electronic signatures are stored in the file to which the signatures is applied. It is not possible to separate the electronic signatures from the file once included. Various checks in each file determine if an electronic signature has been tampered with. If an electronic signature has been tampered with, a symbol is displayed (on electronic display and on printout) indicating the information is false.	Manipulate a digitally signed file with a text editor and access the file with LogTag® Analyzer. Accessing the file is not possible, and a corruption warning message is displayed.	✓

Subpart C - Electronic Signatures

§11.100 General requirements

Requirement	How LogTag® achieves compliance	How we test	Complies
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each user account in the User Server software is identified by a unique username, which is required to access the system. Once a user account is created, the user can not be renamed.	Attempt to generate second account with already existing user name. System does not accept creation of such account. Attempt to rename user account. System does not accept renaming the account.	✓
(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.	Compliance is responsibility of organization implementing this system.	N/A	N/A

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	Compliance is responsibility of organization implementing this system.	N/A	
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.	Compliance is responsibility of organization implementing this system.	N/A	N/A

Requirement	How LogTag® achieves compliance	How we test	Complies
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.	Compliance is responsibility of organization implementing this system.	N/A	N/A

§11.200 Electronic signature components and controls.

Requirement	How LogTag® achieves compliance	How we test	Complies
(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.	Each user must provide a valid username and password to access the system. Users must also provide their correct password each time they add an electronic signature to electronic records.	Log into User Server from LogTag® Analyzer. Both user name and password are required to log in. Digitally sign a file. Password must be re-entered to add the signature.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
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.	Prior to the first signature been performed, the user must gain access to the system using a valid username and password. Each time they add a digital signature, including the first time, the user must provide their current password.	Log into User Server from LogTag® Analyzer. Both user name and password are required to log in. Digitally sign a file. Password must be re-entered to add the signature.	✓
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.	Prior to the first signature been performed, the user must gain access to the system using a valid username and password. Each time they add a digital signature, including the first time, the user must provide their current password.	Log into User Server from LogTag® Analyzer. Both user name and password are required to log in. Digitally sign a file. Password must be re-entered to add the signature. Digitally sign a second, different file. Password must be entered again to add second signature.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
2. Be used only by their genuine owners; and	A user cannot simultaneously access the system from more than one workstation at a time, and only with their logon credentials provided. It is the responsibility of users to keep their access information confidential.	Log into User Server from LogTag® Analyzer. On a second computer, log in with the same user account. Login is refused on the second computer.	✓
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 individuals.	The Administrator of the User Server software cannot discover the current password of a user. It is the responsibility of users to keep their access information confidential.	Log into User Server with admin privileges, open user and try to obtain current password. User Server software does not permit to reveal current password.	✓
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Authorization based upon biometrics is not supported.	N/A	N/A

§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 LogTag® achieves compliance	How we test	Complies
(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.	Each user account within the User Server software is identified by a unique username, which is required to access the system. Each user account has an associated password for the purpose of identifying the user that accesses the system.	Add a user with a given user name, attempt to add second user with same name, User Server software rejects the second name with an error message.	✓
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Users can change their access password at any time, if the Administrator of User Server has granted them permission. The User Server can be configured to force users to periodically change their password. The User Server can also record previously used passwords, encouraging users to use a new password when they update their password.	Set user password expiry to one day, test on next day, LogTag® Analyzer requests password change.	✓
(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.	The Administrator, of the User Server software, can at any time force a user to change the password at the next logon, or disable a user account preventing it being used to access the system, or both.	Change user password, using admin privileges in User Server, and force re-issue. LogTag® Analyzer requests password change when user logs in. Disable user, using admin privileges in User Server. LogTag® Analyzer refuses login for this user.	✓

Requirement	How LogTag® achieves compliance	How we test	Complies
(d) Use of transaction safeguards to prevent unauthorized use of passwords 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.	All failed attempts to gain access to the system are recorded in the audit log file. The User Server will disable a user account if a predefined number of sequential failed attempts have been made. Disabled accounts have a special symbol which is electronically displayed. A user cannot simultaneously access the system from more than one location.	Log on to User Server from LogTag® Analyzer with 3 incorrect passwords. User is now locked, and message in LogTag® Analyzer confirms this.	✓
(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.	Compliance is subject to organization SOP's and their implementation of this system.	N/A	N/A