# 21 CFR Part 11 General Requirements

21 CFR Part 11 requirements when aligned with any regulated system that creates and/or manages the lifecycle of the electronic records and/or digital signatures results in a generic set of requirements that need to be applied and considered across the entire platform.

## System Infrastructure Layer Transaction Requirements

|  |  |
| --- | --- |
|  | All transactions that are executed by users of the system at the infrastructure layer will be recorded and archived in the documented log files, including web server, application server, web service, and directory services. |
|  | All log files created at the infrastructure layers will follow documented naming conventions and archived according to documented requirements. |
|  | All infrastructure access points will be protected with an applicable client authentication method for both user and/or machine access. Exceptions include read-only access to data when that data is documented as being accessible to general internet user communities. |
|  | All infrastructure access points will be protected via SSL, including web server, application server, web service, and directory services. Exceptions include read-only access to data when that data is documented as being accessible to general internet user communities. |

## Structured Data Transaction Requirements

|  |  |
| --- | --- |
|  | The system will record all data transactions that are executed by users of the system at any database layer. Included are transactions that are executed at a relational database, object database, or directory (LDAP) database layer. Transactions should included and record the time the transaction occurred (sysdate), type of transaction (insert, update, delete), and by whom (user ID). |
|  | All database tables will have a corresponding audit table. |
|  | All tables will have corresponding packages and procedures that include preupdate and predelete triggers to capture transactions in the form of records inserted into corresponding audit tables. |
|  | All audit tables will include fields to capture the date and time when auditable transactions occurred (sysdate), type of auditable transaction (update, delete) and by whom (user ID). |
|  | All structured data records that have a corresponding unstructured object should maintain a linkage between structured and unstructured data. |
|  | Access to the structured data repositories (i.e. databases and directories) will be limited to the interfaces created as outlined in supporting requirements documentation for FIREBIRD services. Access through generic client interfaces will be limited to named system administrators under the supervision of documented access controls. |
|  | Updates to data in any structured data repository(s) outside the FIREBIRD services user and machine interfaces must only occur through controlled and documented approaches and only when those modifications are better achieved via native interfaces. |

## Unstructured Data Transaction Requirements

|  |  |
| --- | --- |
|  | All unstructured content objects meta data should include and record the date and time of the transaction occurred (sysdate), transaction type (create, update, delete), and by whom (user ID). |
|  | All unstructured content repositories should facilitate versioning of all unstructured document objects throughout their lifecycle. |
|  | All unstructured content objects meta data should include attributes identified as required or optional such that native ECM technologies and query tools can be used to query, report, and retrieve unstructured content objects. |
|  | Security/access to the unstructured data repositories (i.e. ECM repositories) will be limited to the interfaces created as outlined in supporting requirements documentation for FIREBIRD. Access through generic client interfaces will be limited to named system administrators under the supervision of documented access controls. |
|  | Creation of or updates to objects or data in unstructured data repository(s) outside the FIREBIRD user and machine interfaces must only occur through controlled and documented approaches and only when updates are better achieved via native interfaces. |