

## 4.2 Security issues

LIMS must include certain features for securing the access to the system, the data, and the program files surrounding the system.

**Electronic signature:** The Company plans to use electronic signatures. In order to use E-signatures, there are several security requirements for the rest of the system. The requirements are described in chapter 0 4.2.3 21 CFR Part 11 Compliance.

### 4.2.1 Vision

- Users shall have differentiated access to commands according to their needs and types of jobs or roles they have in the organization.
- Users shall have differentiated access to which data they are allowed to see, use, change, and maintain.
- Labs like i.e. Microbiological Control Laboratory which test on all types of samples shall have access to their samples for results entry, but not to other parts of the same samples, which 'belong' to other groups.
- Nobody shall have access directly to the Oracle database uncontrolled by LIMS for viewing, updating, writing to, and deleting data.
- Files where LIMS data or LIMS programs are stored shall have restricted access.
- All changes in LIMS shall include an audit trail giving information on who made the change and when it was made and a mandatory reason to be given explaining why the change was made. The reason shall be chosen from a list.
- Old versions of template parts and data shall not be deleted, but given a different status ('old / replaced').
- The LIMS security system is good enough for the 21 CFR Part 11 Electronic data and Electronic Signature.

### 4.2.2 General security issues

| ID      | General Security Requirement Text   | Answer | Reference |
|---------|---|--------|-----------|
| 4.2.2.A | Explain how access to functions and data is handled in the LIMS   |        |           |
| 4.2.2.B | Explain how access directly to the database can be limited  |        |           |
| 4.2.2.C | Which users must have direct access to the LIMS database (not through LIMS)   |        |           |
| 4.2.2.D | Explain how version control and audit trails are handled for the data in LIMS, both for the template part and for the part that covers the daily use. |        |           |
| 4.2.2.E | Files needed by LIMS stored on the server. Explain who needs direct access to these, and how the access can be limited to a minimum of persons.       |        |           |
| 4.2.2.F | In which cases are old data automatically deleted by LIMS?  |        |           |
|         | <b>Access levels:</b>   |        |           |
| 4.2.2.G | Each user has his /her own access with combinations of commands and datagroups (See also 0 4.2.3.1 Electronic Records)                                |        |           |
| 4.2.2.H | No user has access to commands / datagroups that are not defined for the user (See also 0 4.2.3.1 Electronic Records)                                 |        |           |
| 4.2.2.I | Access to commands shall not be preset in the system, but be configured to the laboratory's needs.  |        |           |

| ID      | General Security Requirement Text  | Answer | Reference |
|---------|--|--------|-----------|
| 4.2.2.J | Change in access shall be easy to make for users who can change other users access rights.         |        |           |
| 4.2.2.K | Only system manager and a superuser shall have access to the entire LIMS (database, NLS files etc) |        |           |

## 4.2.3 21 CFR Part 11 Compliance

### 4.2.3.1 Electronic Records

| ID        | 21 CFR Part 11 Requirement Text   | Answer | Reference |
|-----------|---|--------|-----------|
|           | <b>§11.10 General requirements</b>  |        |           |
| 4.2.3.1.A | LIMS can discern invalid records  |        |           |
| 4.2.3.1.B | LIMS can discern altered records  |        |           |
| 4.2.3.1.C | LIMS can generate accurate and complete copies of records in human readable (paper) form for inspection, review, and copying                                      |        |           |
| 4.2.3.1.D | LIMS can generate accurate and complete copies of records in electronic (Floppy disk, CD, ASCII, pdf) form for inspection, review, and copying                    |        |           |
| 4.2.3.1.E | LIMS can protect records to enable their accurate and ready retrieval throughout the records retention period   |        |           |
| 4.2.3.1.F | Limitation of system access to authorized individuals, each with their own, individual account  |        |           |
| 4.2.3.1.G | Audit trail is automatic and computer generated   |        |           |
| 4.2.3.1.H | Audit trail is date stamped day-month-year  |        |           |
| 4.2.3.1.I | Audit trail is time stamped hour-minute-second in locally defined time  |        |           |
| 4.2.3.1.J | Audit trail includes full name of the operator, or LIMS-defined operator ID   |        |           |
| 4.2.3.1.K | Audit trail records all system activity   |        |           |
| 4.2.3.1.L | Audit trail records all user logons and failed logons   |        |           |
| 4.2.3.1.M | Audit trail is generated during creation of data  |        |           |
| 4.2.3.1.N | Audit trail is generated during modification of all data  |        |           |
| 4.2.3.1.O | Audit trail is generated during 'deletion' or 'deactivation' of all data  |        |           |
| 4.2.3.1.P | If the record is changed the system retains/displays old/new value  |        |           |
| 4.2.3.1.Q | Changes to electronic records shall be made without obscuring previously recorded information (i.e. new versions are created instead of overwriting old versions) |        |           |
| 4.2.3.1.R | Changes shall be accepted only when the user has stated a reason for the change   |        |           |
| 4.2.3.1.S | Reasons for changes shall be picked from a pre-defined list of valid reasons  |        |           |
| 4.2.3.1.T | Reasons may additionally be typed-in by the user if the list does not contain correct reasons   |        |           |
| 4.2.3.1.U | Audit trail associated with the record  |        |           |
| 4.2.3.1.V | Audit trails are available for review and copying by regulatory authority   |        |           |
| 4.2.3.1.W | Operational system checks enforce permitted sequencing as appropriate   |        |           |

| ID        | 21 CFR Part 11 Requirement Text   | Answer | Reference |
|-----------|---|--------|-----------|
| 4.2.3.1.X | Authority checks are designed to ensure that only authorized individuals can perform various tasks in the system. |        |           |
| 4.2.3.1.Y | The system is able to discern the validity of the source of input   |        |           |