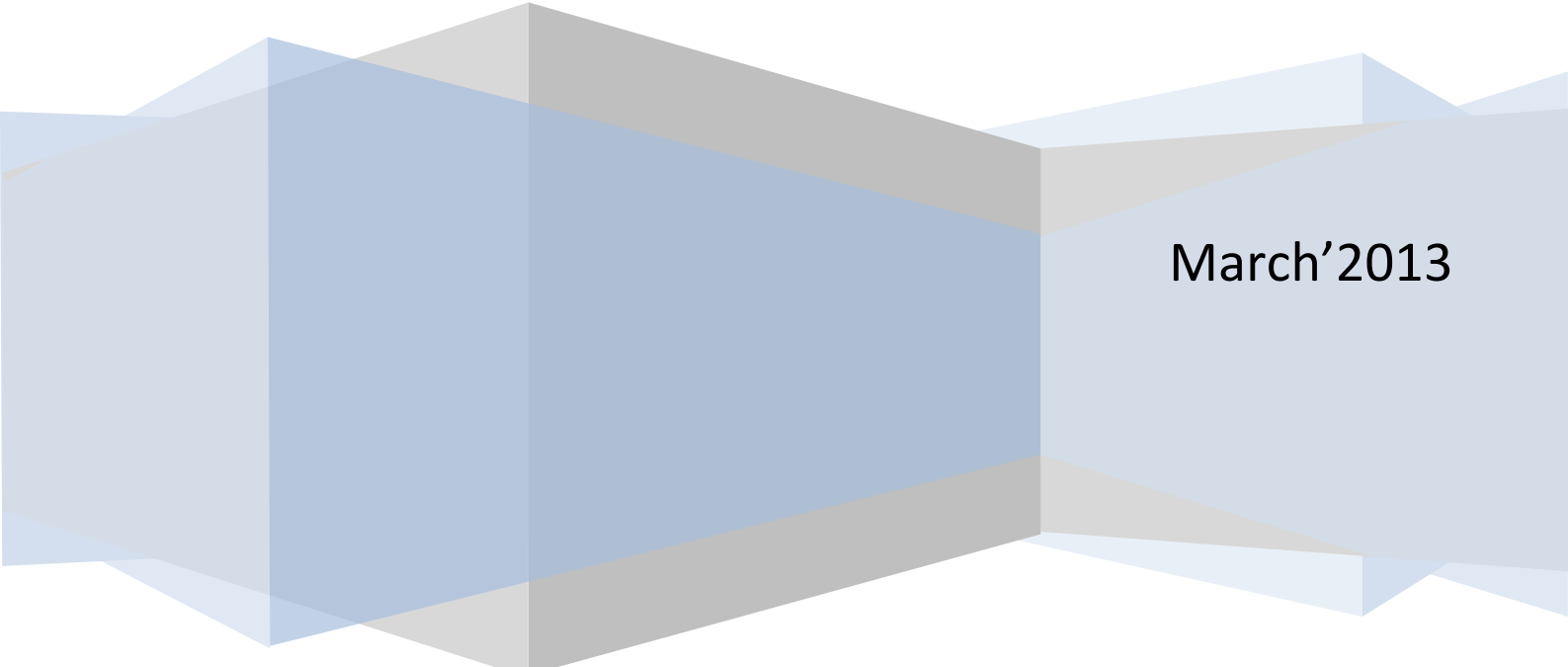


**Busysoft Systems Private Limited**

**Implementation of ISO-15189 Recommendations for protection of  
laboratory information systems (LIS) Annex 'B'**

# **Labmate.net ERP LIMS**



March'2013

**Implementation of  
ISO-15189 Recommendations for protection  
of laboratory information systems (LIS) Annex 'B'**

**Labmate.net ERP LIMS**

Manual Version: 1.5

Date of Issue: 2013/03

Manual Code: UG/11

We reserve the right to make changes in the course of technical development without previous notice. Neither this manual nor any parts of it may be duplicated or transmitted in any way without the written approval of Busysoft Systems Private Limited.

© 2010 Busysoft Systems Pvt. Ltd. All rights reserved.

New Delhi, India

[www.busysoft.in](http://www.busysoft.in)

## Trademarks

**Labmate.net ERP, Labmate, and Busysoft** are trademarks of Busysoft Systems Private Limited. All other trademarks names used in this manual belongs to other companies are hereby acknowledged.

## Software Copyrights

**Labmate.net ERP LIMS** Software of Busysoft Systems Private Limited is the copyright property of Busysoft. All rights to this software are retained by Busysoft. You are entitled to use this software as well as the printed documentation relating to it on one single, non-transferable workstation.

## Disclaimer

Busysoft Systems Private Limited has validated the provided instructions, instrument, software and customizable features for this system to optimize product performance and meet product specifications. User defined modifications are not supported by Busysoft as they may affect performance of the system. It is the responsibility of the user to validate any modifications made to these instructions, instruments, software provided by Busysoft.

## Version Date Changes

Sr.No.	Manual Version No.	Date of issue	Manual code
1	1.1	2010/07	UG/11
2	1.2	2011/02	UG/11
3	1.3	2012/03	UG/11
4	1.4	2012/10	UG/11

We reserve the right to make changes in the course of technical development without previous notice.

Neither this manual nor any parts of it may be duplicated or transmitted in any way without the written approval of Busysoft Systems Private Limited.

© 2010 Busysoft Systems Pvt. Ltd. All rights reserved.

New Delhi, India

[www.busysoft.in](http://www.busysoft.in)

## **Introduction**

The guide contains the guidelines for implementation of ISO-15189 recommendations for protection of laboratory information systems (LIS). These guidelines are given as annex B. All the guidelines are mentioned point wise in this document. The implementation and compliance of each aspect of guideline in Labmate.net ERP are given in blue color.

A special section has been devoted to few industry standard guidelines at the end of the document. The contents are reference material available on internet.

## Annex B

### (Informative)

## Recommendations for protection of laboratory information systems (LIS)

### B.1 General

B.1.1 Results and information are the products of the medical laboratory. Because computer systems can be damaged or subverted in a variety of ways, it is important to establish policies that protect patients from harm caused by loss or change of data.

The recommendations given in this annex ought to result in a high level of data/information integrity for laboratory information .

NOTE They are not applicable to

- Desktop calculators,
- Small programmable technical
- purchased services and
- Computers used spreadsheets or similar, single-user functions
- dedicated microprocessors that are an integral part of an examination instrument.

### B.2 Environment

B.2.1 The computer facilities and equipment should be clean, well maintained and location and environment that complies with vendor specifications.

- These are internal procedure/functions/requirements/environment of the Laboratory.
- Keep the servers in separate air-conditioned room. The access control to the room should be monitored. The servers should be kept on table or inside a server cabinet as per the vendor specifications. Proper ventilations and air flow should be maintained for heat dissipation. A general guideline regarding the server room is given below in separate document.

B.2.2 Computer components and storage areas should be readily accessible to appropriate fire-fighting equipment.

- These are internal procedure/functions/requirements/environment of the Laboratory.

B.2.3 Wires or computer cables should be protected if located in traffic areas.

- These are internal procedure/functions/requirements/environment of the Laboratory.

B.2.4 There should be provision for an uninterruptible power supply (UPS).

- These are internal procedure/functions/requirements/environment of the Laboratory.

B.2.5 The information facilities should be protected from unauthorized access.

- These are internal procedure/functions/requirements/environment of the Laboratory.

### B.3 Procedure manual

B.3.1 A complete computer procedure manual, which may be electronic, should be readily available to all authorized computer users.

Does the LIMS has proper installation guide:

Does the LIMS has Users operations Guide:

Does the LIMS has online manual:

Does the LIMS has Help manual :

Labmate.net ERP LIMS has following manuals

- Installation Guide: The installation guide contains 40 pages. The manual contains defined procedures for installation of software on server and terminals.
- User's Guide: For Daily operations and maintenance
- Data maintenance guide

The chapters are as per the Labmate.net ERP LIMS screen functions. The manual explains each screen, associated functions, procedures and buttons.

B.3.2 The laboratory computer procedure manual should be reviewed and approved at defined intervals by the laboratory director or a person designated for this task.

- These are internal procedure/functions/requirements/environment of the Laboratory.

B.3.3 There should be written procedures for actions necessary to protect the data or computer equipment or both in case of fire or hardware/software failure.

Does the LIMS has data backup facilities:

Does the LIMS provides Restore facilities:

Does the LIMS has written procedure for data manageability:

The Labmate.net ERP LIMS User's Guide provides complete details about data maintenance procedure. It contains sections on Data backup and Restore. The software can predefine the data back duration. The user can take data back up

-Automatically

-Manually

-Optionally

The software prompts the user on the above basis and takes the backup as soon the application starts.

### B.4 System security

B.4.1 Computer programs should be adequately to prevent alteration or destruction by casual or unauthorized users.

- The Labmate.net ERP LIMS software program is secured and runs on the windows 2008 R2 operating system. The software works in a domain networking environment. Domains are managed centrally by using domain controllers and provide a higher level of security and control over users and computers. You could group users and computers and then manage those using policies which dictate things such

as which group of users are able to access certain resources or perform some specific task which needs elevated privileges or the logon times. Also, over the time as your infrastructure expands, you could divide your domain into subdomains and delegate the administration duties to other administrators to manage their subdomains. This policy does not allow the casual users or unauthorized to alter and destruct any content from the system.

B.4.2 Strict policies should be established for authorizing use of the computer system. Policies should define those authorized to access patient data and those authorized to enter patient results, change results, change billing or alter computer programs.

Does the LIMS provide facilities to protect data from unauthorized alteration?

Does the LIMS provide facilities of data audit?

Does the LIMS provide data protection facility?

Does the LIMS provide data rollback procedures?

Does the LIMS provide facilities to protect data from deletion?

**Authorize access:** The software provides security access to each and every user. The user logs in using a unique user ID and password. All the activities done by the user are logged against the user. Each activity can be allowed or disallowed and can be set by the Administrator (Manager). Audit can also be done on these activities carried out by the user to monitor.

**Data Modification Log:** The patient results entered by a user are monitored and are kept on the basis of each modification. The modified results can be checked for any patient. All the activities done by the user are logged against the user name and are stored in a log file. The log file is available only for Manager or Administrator. The user activities such as patient deletion, Cancel, report modifications, deletions, and duplicate report print can be specifically monitored and the log can be viewed and printed.

**The data is protected at three levels**

a. System Level: Use Windows authorization process at networking level

- This provides access to Server at disk and file level
- Use Windows servers 2008 R2 or above to provide the same.

b. Data Base level: The Labmate.net ERP LIMS uses MS-SQL 2008 R2 database management system. This software provides security access to each and every user. The user can use the software by a unique user ID and password. The activities can be specifically can be allowed or disallowed.

c. Software level: The Labmate.net ERP LIMS software provides security access to each and every user. The user can use the software by a unique user ID and password. The activities can be specifically can be allowed or disallowed.

- Add
- Modify
- Delete
- Copy
- Print

B.4.3 If data in other computer can be accessed through the LIS (e.g. pharmacy or medical records), there should be appropriate computer security measures to prevent unauthorized access to these data through the LIS. The LIS should not be allowed to jeopardize the data security of other systems.

Labmate.net ERP LIMS (LIS) system accesses the other systems data such as Hospital information systems (HIS)

- ☑ **Using Proprietary data retrieval:** Labmate.net ERP LIMS software only reads the required information and does not write back any information. HIS or other such software can also retrieve the required information from Labmate.net ERP LIMS LIS. This is done using [views](#) in MS-SQL.
- ☑ **Using export import files:** Labmate.net ERP LIMS reads the exported information (From other Healthcare applications) from CSV formats (or other such formats) into its database and also can write back the required information in CSV formats for use by other healthcare applications.
- ☑ **Using HL7:** All required information is sent or received using HL7. The sending or receiving application decides about its use and inserts the information itself into its database. No direct data access is provided to the applications.

## B.5 Data entry and reports

B.5.1 Patient data on reports and video displays should be compared with original input in order to ensure the integrity of data transfer at defined intervals by detecting errors in data transmission, storage or processing.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The Labmate.net ERP LIMS software provides a facility to view the reports and record the checking procedure by an authorized user. All the checking done by the user is recorded and can be monitored. Any alteration done by the users can be monitored at any time.

B.5.2 Whenever multiple copies of tables are maintained within a system (e.g. biological reference interval tables in both the laboratory information system and the hospital information system), they should be periodically compared in order to ensure consistency among all copies in use. Appropriate replication or comparison procedures should be in place.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.5.3 Documentation should exist stating that calculations performed on patient data by the computer are periodically reviewed.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.5.4 The LIS output to the medical record constitutes direct patient-care data. Accordingly, the laboratory director should approve and review the content and format of the laboratory reports in order to ensure that they effectively communicate laboratory results and meet the needs of the medical staff.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.5.5 Data entered into the computer system either manually or by automated methods should be reviewed in order to verify the correctness of the input data before final acceptance and reporting by the computer.



- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The Labmate.net ERP LIMS software provides a facility to view the reports and record the checking procedure. The reports entered into Labmate.net ERP LIMS can come from Labmate.net ERP LIMS Interface (automated) or manually.

**Automated reporting:** The results are transferred from analyzer to patient report. The interface program has a facility to accept or reject the data before releasing results into patient reports. Retesting using new sample or same sample can be done at this stage.

**Manual reporting:** The manual data can be entered into the system.

Software provides a three level of checking and verification.

**Checking:** The data is checked for correctness by comparing it with manual register or analyzer printout if required. The checking can be done by only authorized user. The reports which are checked can only move further for authentication and releasing.

**Provisional Authentication:** All the reports need to be provisionally authenticated. This is the second level of checking. The reports which are provisionally authenticated can only move further for authentication and releasing.

**Final authentication:** All the reports need to be Final authenticated. This is the third level of checking. The reports which are final authenticated can only move further for releasing.

B.5.6 All result entries should be checked against a predefined range of values for a particular examination in order to detect absurd or impossible results before final acceptance and reporting by the computer.

The Labmate.net ERP LIMS keeps details of all predefined range of values and interpretation for each test on the basis of Age, Sex, for each analyzer/reagent, and date of using the value. The values contained are

**Reference ranges:** These are predefined reference ranges for various ages and sex.

**Panic ranges:** These are predefined panic ranges for various ages and sex.

**Threshold ranges:** These are absurd and impossible result ranges or various age and sex.

The Labmate.net ERP LIMS software detects the issues and warns with color coding at the time

- ☑ Analyzer Interface result view
- ☑ Patient report feeding
- ☑ Checking
- ☑ Authentication

B.5.7 The reporting system should provide for comments on sample quality that might compromise the accuracy of examination results (e.g. lipaemic, haemolyzed samples) and for comments on interpretation of results.

- ☑ The reporting system special comments can be inserted for each test. These comments can contain sample quality or any other observations made on interpretation of results. These are user defined comments.

B.5.8 There should be an audit mechanism allowing the laboratory to identify all individuals who have entered or modified patient data, control files or computer programs.

The Labmate.net ERP LIMS software allows the software usage only on proper authentication login. Once the user logs into the system, its activities are recorded throughout the system for:

- Additions
- Modifications
- Deletions

The activity details kept by the system are

- Date and time of activity
- User Id
- System IP address

These can be used for establishing the trail.

## **B.6 Data retrieval and storage**

B.6.1 Stored patient result data and archival information should be easily and readily retrievable within a time frame consistent with patient-care needs.

- Labmate.net ERP LIMS system provides backup and restore facilities to retrieve the required data. The authorized user can select the archived database for easy retrieval of required information.

B.6.2 The computer should be reproduce archived examination results, including the interval originally given for an examination and any interpretative comments attached to the result, as well as the of measurement at the time the measurement was made.

- The Labmate.net ERP LIMS keeps details of all predefined range of values and interpretation for each test on the basis of Age, Sex, for each analyzer/reagent, and date of using the value. The values contained are

**Reference ranges:** These are predefined reference ranges for various ages and sex.

**Panic ranges:** These are predefined panic ranges for various ages and sex.

**Threshold ranges:** These are absurd and impossible result ranges or various age and sex.

The Labmate.net ERP LIMS software stores the applicable reference range details into the patient record. The reference range once used into the patient record cannot be deleted or modified. The same reference range is then printed given each time the patient report is printed.

B.6.3 Patient and laboratory data should be retrievable, “on-line”, for a designated period of time on depending on the needs of the individual organization.

- Labmate.net ERP LIMS online module provides all the facilities of retrieving data “on-line” as and when required.

B.6.4 Data-storage media such as tapes and disks should be properly labeled, from damage or unauthorized use.

- These are internal procedure/functions/requirements/environment of the Laboratory.

B.6.5 Efficient back-up should be in place to prevent loss of patient result data in case of hardware or software failure.

- Labmate.net ERP LIMS data backup and restore can be done two ways. Please follow data maintenance guide for instructions.
  - Using MS-SQL 2008 R2
  - Using Labmate.net ERP LIMS maintenance software
  - Recommended to have separate storage location for the back-up data as per policies of the IT department.

B.6.6 Computer alarm systems (usually the main computer console that monitors hardware and software performance) should be monitored and tested regularly to ensure their proper functioning.

- Alarm System on UPS Battery status / Ups time left/UPS battery Down:** The UPS come with a UPS management software. The pc is connected with the UPS using a RS232 serial cable. The UPS software supplied by the company (UPS Company) keeps track of all the warnings regarding the UPS status.
- Alarm system on Hard disk usage:** The Hard disk management system (Available in Operating system) keeps track of this warning. You can buy third party tools as well such as Norton Disk Manager.
- Alarm system on database management system (Alarm on backup due and alarm on database maintenance due):** The database management system (such as MS-SQL) can take care of the same. Other backup software such as Seagate backup etc. can take care of such provisions.
- Alarm on Virus detection/Alarm on Virus attack:** Buy firewalls, Internet security, and Antivirus software to deal with the same.
- Alarm on unauthorized access:**
  - Alarm on unauthorized access on LAN
  - Alarm on unauthorized access on Wireless LAN
  - Alarm on unauthorized access of information
  - Alarm on unauthorized changing of system parameters

## B.7 Hardware and software

B.7.1 A written procedure and a complete record of all preventive maintenance for all computer hardware should be readily available.

- These are internal procedure/functions/requirements/environment of the Laboratory.
- It is done using Labmate Asset Management System, where all records of equipment and preventive maintenance are kept.

B.7.2 The system should be checked after each back-up or restoration of data files in order to ensure that no inadvertent alterations have occurred.

- These are internal procedure/functions/requirements/environment of the Laboratory.
- Appropriate Backup software, devices should be installed to check the redundancy.

B.7.3 Mistakes detected during system backup should be documented, along with corrective action taken, and reported to the responsible person in the laboratory.

- These are internal procedure/functions/requirements/environment of the Laboratory.
- The documentation can be done manually or can be done in Labmate NC/CAPA software program. Each issue can be documented in details along with actions taken by the responsible persons.

B.7.4 Any alterations to the system hardware or software should be verified, validated and completely documented in order to confirm that changes are acceptable and appropriate.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The hardware and software requirements for the Labmate.net software are well defined. The resources may change over time period but should be validated as per the recommendations.
- ☑ The documentation can be done manually or can be done in Labmate NC/CAPA software program. Each issue can be documented in details along with actions taken by the responsible persons.

B.7.5 The laboratory director or person designated for the task is responsible for the accurate and effective delivery of examination results to the requesting clinician and should approve all changes in the computer system that may affect patient care.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.7.6 Programs should be checked for proper performance when first installed and after changes or modifications have been made.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The IQ, OQ, PQ documents are provided with the checklist of the functions to be checked for proper performance.

B.7.7 The purpose of a program, the manner and its interaction with other programs should be clearly stated. The degree of detail should be adequate to support any troubleshooting system modification or programming – as applicable – done by the computer operators.

- ☑ The Labmate.net ERP LIMS software pre installation, installation and implementation manual give details about the software and hardware requirements for Labmate.net ERP LIMS. These manuals also specify operating system requirements, Database management system requirements, specific software and hardware tools, software controls and their installation procedures.

B.7.8 Those interacting with the computer system should be taught how to use a new system or modifications of the old system.

- ☑ Labmate.net ERP LIMS Training Program: Labmate.net ERP LIMS provides training to the Labmate.net ERP LIMS users. The Labmate.net ERP LIMS users are provided a training schedule according to which they are taught to use Labmate.net ERP LIMS effectively.

B.7.9 The laboratory should have responsible person to whom all significant computer malfunctions are to be promptly reported.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The documentation can be done manually or can be done in Labmate NC/CAPA software program. Each issue can be documented in details along with actions taken by the responsible persons.

## B.8 System maintenance

B.8.1 'Downtime' for maintenance should be scheduled to minimize interruptions of patient-care service.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.
- ☑ The system provides a procedure of backup and restore of the data. In case of system emergency data can be restored onto the backup systems.

B.8.2 There should be documented procedures for handling the shutdown and restarting of the system in order to ensure integrity of the data, uninterrupted delivery of laboratory services and proper functioning of the system after restarting.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.8.3 There should be written procedures for handling downtime on other systems such as the hospital information system, to ensure the integrity of patient data. Procedures for verifying recovery of the other system and the replacement or updating of data files should be available.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.8.4 All unscheduled computer downtime, periods of system degradation (response time) and other computer problems should be documented, including the reasons for failure and the corrective action taken.

- ☑ Labmate.net ERP LIMS Provides a NC/CAPA module (Optional) which keeps tracks of all Nonconformance / Corrective Action and Preventive Action. All the users can record the issues related to the problems, suggestions into the system. The administrator can evaluate and take corrective actions and close the issues.

B.8.5 Written contingency plans should be developed to handle services in the event of a computer system failure such that patient results are reported in a prompt and useful fashion.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

B.8.6 Records should be maintained that document regular maintenance and allow operators to trace any work done on the computer system.

- ☑ These are internal procedure/functions/requirements/environment of the Laboratory.

## Server Room

**Acknowledgements:** <http://www.wikihow.com/Design-a-Server-Room>

A server room is the physical space that houses all the data running through the computer network of a business or organization. Most Information Technology professionals spend a lot of their time there, troubleshooting server or network issues and performing routine maintenance. Putting together a safe and accessible data center for the storing of technology and files is essential in creating a hub for IT infrastructure and operations. Design a server room that is safe, spacious and computer friendly for the entire IT team.

The server room should be kept separate from working environment of IT people. They should visit the room only for maintenance, trouble shooting and cleaning purposes. Do not attach working peripherals such as printers, scanners with the server. Using these peripherals with the server affects the performance. Do not run applications and additional services on the server. The data servers and application servers should be kept separate for all the applications for better performance.

### Steps

**Determine the appropriate room size.** Physical space needs must be decided before any further details are incorporated into the server room. There needs to be enough room for the servers, wires, cables, and other necessary equipment. Data should be kept away from an exterior wall, if possible.

**Set up hardware for storage.** For space maximization, utilize cabinets and shelving to store the physical machinery and other computer inventory in the server room. Telco racks are popular in many operational spaces, and a single rack can hold hundreds of 1U high servers and blade servers.

**Keep the room cool.** A proper server room needs to stay cool and dry to keep all of the equipment from overheating. One option is to install a raised floor to distribute cooling. Another option is to use in-row cooling units, which do not require a raised floor and move the compressor to the roof. You may want a ceiling that is at least 12 to 18 feet (3.7 to 5.5 m) high. Keep a thermometer in the room to ensure the temperature is moderate. A dehumidifier may be necessary if the room gets too humid.

**Make space for cables.** A server room should have enough space under the floor to run electrical cables. Have an electrician install power whips from 1 central electrical panel. This cuts down on the electrical services being routed to each individual fixture.

**Develop security procedures.** The server room should be restricted to only the people who need to go there to do work. Keep it locked, or install a handprint or fingerprint recognition system. A secure server room is essential for data protection.

**Allow for monitoring.** The server room should be monitored around the clock. All activity coming over the network servers should be scanned for abnormalities. Software exists to allow for notifications to pagers, or cell phones and emails if the monitoring reveals anything alarming.

### Tips

- Remember to plan for growth. When designing the server room to accommodate the current IT needs, keep in mind that the business and the technology will likely grow. Leave enough room for the anticipated growth, so that all the necessary files and information can be kept in one place.

- Keep cabling up to fire codes. Run cabling that is at least Category 6 to ensure safe and speedy network services. Consider having the cabling installed professionally, and it will usually come with a warranty of 5 to 10 years.

#### **Things You'll Need**

- Cabinets
- Shelving
- Telco racks
- Thermometer
- Cables
- Locks
- Security system

## Six tips to help design a server room for speed and security

By Scott Lowe MCSE

January 24, 2002, 8:00am PST

It's inevitable. At some point in your IT career, you'll be doing your job, minding your own business, and it will hit you: You're running out of space in your server room. Or maybe your company or group will move to a new location. In any case, you may be called on to design a new data center for your environment. While this is definitely a lot of work and requires careful planning, the end result can be a center that is built for speed, is secure, and that can grow to accommodate future needs.

In this Daily Drill Down, I'll provide some tips that will aid you in designing your server room, the hub of your IT infrastructure, so that it will not only fit your current operational needs, but it will also be expandable, secure, and built for speed.

### 1. The basics

You must consider some basic design decisions before you begin construction of a new data center. First is physical location and room size. When possible, keeping your data away from an exterior wall will generally provide for more security. When it comes to size, plan for growth. The chances that you'll need to grow your infrastructure are pretty good, and you'll probably want to keep all of your equipment in one location.

Hardware capacity in a server room is usually the prime factor when determining space. Space is expensive and you want to get the best possible return on your investment. Many organizations use telco racks or enclosed cabinets to make the most of the space they have. Today, with 1U high servers and new blade servers, you can pack anywhere from 42 to hundreds of servers in a single rack.

---

### Measuring the Us

1U is approximately two inches, and 2U is approximately four inches.

---

Planning for space under a raised floor and a ceiling from 12- to 18-feet high will go a long way toward creating a server room that can be properly cooled and maintained. A higher ceiling allows for more tolerance in the event that the room begins to overheat. Having space under the floor to run cables is critical for rooms of almost any size. It also allows you to use power whips from a central electrical panel rather than having to use a fixed outlet. I much prefer to use power whips since I can run them wherever I want under the floor and can easily add a custom whip of a different rating for equipment with special needs.

---



## Power whips?

Power whips are armored wire cables that are factory-installed so an electrician can connect multiple fixtures to one centralized junction box. This keeps the electrician from having to bring electrical service to each fixture.

---

## 2. Security

For data security, keeping up with service packs, patches, and locking down systems only goes so far. Every security plan also needs to address the physical security of the hardware housing the data and of the infrastructure passing the data. Keeping up with every patch from every vendor will do nothing if someone can walk into your server room and mess with your hardware or walk out of the building with it.

First on the list for security is a strict policy only allowing people who need to be in the room to enter. Using a system such as a keycard with time restrictions is another way to keep track of who is entering and leaving the room and when. Other, more advanced, systems will make your environment even more secure. For example, you could install a handprint recognition system or a system that weighs people on their way into and out of the room to make sure that equipment is not being removed without authorization. It all depends on how much security you require and how much you are willing to spend on it.

---

### Handprint recognition

Looking for a handprint recognition system? Take a look at the [Biometric Consortium](#) for more details.

---

Another aspect of your security plan is the installation of devices to protect your investment, such as fire detection and suppression systems and water detection systems, depending on where your server room is situated. At one point in my career, I found out how important a water detection system can be. On the floor above the central network hub that served ten buildings, a water problem resulted in gallons of water being filtered by a device that was *not* designed for water filtering—my network backbone switch. While a water sensor wouldn't have prevented the actual water problem, it could have allowed me to move the switch before more damage was done.

---

### Water sensors

If you're looking for a water sensor, take a look at [these](#) Google results and take your pick.

---

## 3. Environment

When thinking about physical security for your new data center, also consider other environmental factors. Some of these will only appear on your to-do list if you live in certain areas of the country:

- Severe weather—tornados, hurricanes, or frequent, severe lightning storms
- Earthquakes
- Flooding
- Dry conditions, which increase fire potential

Keeping your server room within environmental limits set by the various manufacturers is absolutely critical to maintaining a reliable, highly available infrastructure. Plan how you will maintain a reasonable temperature and humidity level and supply the appropriate power to the room. As I stated, I like to have the power connections run under the floor on flexible cables. This allows me to place them wherever I need them and to install special power connections, such as a 230-watt whip, if needed. Consider a UPS that can carry the load of all of the critical components of the room for an extended period of time. If you're running a mission-critical environment, consider a generator that can back up the UPS in the event of a prolonged outage. In addition, procuring power supplies from more than one provider is an important step in ensuring the full-time operation of your environment.

#### 4. Monitoring

Often an overlooked component to maintaining a reliable infrastructure, monitoring's importance cannot be overemphasized, especially if you maintain a 24/7 environment. From the beginning, you should plan on setting up systems to monitor every possible aspect of your environment, from servers to network components to monitoring your network traffic. Most monitoring software will allow for notifications to pagers, etc., and I recommend that you take advantage of them. If you'd like to find a low-cost monitoring solution that will cover much more than the basics, take a look at Big Brother and MRTG.

---

#### Big Brother and MRTG

If you want information on Big Brother and MRTG, see the following articles: ["Big Brother is watching your network"](#) and ["Enhance MRTG's network graphing with the Round Robin Database Tool."](#)

---

In addition, you should evaluate software packages that can help you protect your data against outside attacks and that verify the integrity of your hardware security solutions, such as firewalls.

#### 5. Cabling for speed and flexibility

One major consideration in the design of a server room is the speed of the connections that it will support. My recommendation: Make it as fast as you can afford. I have seen organizations "low ball" the cabling in a server room only to regret it very soon thereafter. In addition, make sure that all cabling is up to fire codes. It may be a little more expensive initially, but it's much less expensive than having to replace the cabling and, of course, you can't compare the cost of the cable to the cost of a life that may be saved by using the proper cabling.

Inside the server room, you should run nothing less than category 6 cabling if you're building it from scratch. I recommend having the cabling professionally installed by an organization that will certify and give a warranty for its work. Many cabling plants can be guaranteed for five or ten years, potentially saving you a significant amount of downtime and money in the event of a problem with the cable plant. During this process, make sure that your cabling plant is capable of gigabit speeds.

If you have room in the budget, you should also seriously consider fiber runs to strategic points in your server room. The capacity of fiber is much greater than that of copper, and installing it during an initial cabling project is generally less expensive than installing it piecemeal after the fact.

For facilities that include remote cabling closets, run both single and multimode fiber to the remote locations, and a few copper runs to provide the maximum flexibility. You never know what you'll have to support down the line.

When considering speed, it's also important to consider how fast new hardware can be rolled out. As I discussed before, a rack-based solution can ease this burden significantly, but it also has other benefits.

Consider a situation in which you may want to reorganize your server room. In a recent server room design, I ran 24 pairs of plenum category 6 cables under a raised floor back to a central network switch from an enclosed cabinet filled with servers. When this cabinet had to be moved to a new location, it was fairly simple. I disconnected the D connector on the end of the cable pair, as well as the power connections to the rack (of which there were six), moved the cabinet, and reconnected the cables. Job done.

Where possible, cable pathways should be provided under the floor to keep it from becoming a tangled rat's nest, which is all too common in many environments. A rat's nest can present problems during troubleshooting when a cable needs to be traced through the mess. This can result in extra downtime and has the potential to cost your organization more money.

#### 6. Keep the big picture in mind

During the design phase, consider the effect that each of your design decisions will have on your business and determine whether a particular investment is worth the cost. For example, is uptime critical enough to your business operations to warrant the cost of a backup generator to provide power? When considering the costs of downtime, remember that many factors must be considered, such as staff costs to recover from the outage, employee downtime, lost sales, and poor publicity.

#### Conclusion

The day after you're finished building your server room, complete with sufficient power whips under 12 inches of raised floor, 18-foot ceilings, adequate heating and cooling and humidity control, and a complete monitoring solution, you'll be asked to add something new. If you build your server room properly, this should be a painless process. If you use rack-based servers and get the cabling piece done ahead of time, adding a server to the rack should be a piece of cake and leave you only with the task of adding a new server to the monitoring system.

With some careful planning and a forward look at both technology and your enterprise, your new server

room can be built so that it's secure, flexible, and can allow everything to be done quickly—from transferring data at multi-gigabit speeds to setting up a new server in minutes.

**Implementation of  
ISO-15189 Recommendations for protection  
of laboratory information systems (LIS)**

**Labmate.net ERP LIMS**

Manual Version: 1.5

Date of Issue: 2013/03

Manual Code: UG/11

We reserve the right to make changes in the course of technical development without previous notice. Neither this manual nor any parts of it may be duplicated or transmitted in any way without the written approval of Busysoft Systems Private Limited.

© 2010 Busysoft Systems Pvt. Ltd. All rights reserved.

New Delhi, India

[www.busysoft.in](http://www.busysoft.in)

[www.busysoftsystems.com](http://www.busysoftsystems.com)