# IT POLICY SMS LUCKNOW

## 1. ACCOUNT AND PASSWORD MANAGEMENT POLICY

The following procedures are in computer labs to manage the student user accounts in secure manner:

- "Student" will be the user's name /password for all students to access the computers in computer labs.
- Students having user name and password with limited privileges to prevent the configuration changes of network systems.
- All the cookies and remember passwords will be removed in system profile and web browsers during the preventive maintenance schedule in computer labs.
- Students should ask the concern lab technicians to reset the password if they forgotten or security breach unfortunately.
- Students should not share their login passwords to anyone to prevent data loss or misuse their accounts.

The following procedures are followed in departments to manage the staff user accounts in secure manner.

- admin will be the user's name for staff to access the Internet in our institution. Staff can change their password during the first login attempt.
- Sharing folder in server can be access by the authorized staff members to update the academic and administrative data.

The following procedures are followed in our campus to manage user accounts for IT helpdesk:

- Administrator account of all ICT devices should be reset at the time of installation.
- User account and passwords will be reviewed and changed in all servers at periodic intervals.

The following security precautions should be followed by students and staff to manage their user accounts in secure manner.

- Strong alphanumeric passwords should always be used to protect administrator accounts and end user account by using one upper case, one lower case letter and special symbols.
- Passwords for new accounts should NOT be emailed to remote users.
- Passwords must not be stored in clear text or in any easily reversible form m easy access areas.
- Passwords should not contain the first name of staff or equipment

Director
School of Management Sciences
Lucknow

## 2. WIRED AND WIRLESS NETWORK ACCESS POLICY

The following guidelines are followed to wired network to enrich the performance and speed of network connectivity:

- Network connectivity provided to all blocks of the Institution on authenticated network access through fiber optics and Layer-2 switch connectivity.
- Any desktop or server that will be connected to the network is configured with unique IP address assigned by the IT helpdesk.
- File and data sharing facilities on the computer over the network is protected with user name and password with appropriate access rules in Proxy server.

The following guidelines are followed to wireless network to enrich the performance and speed of network connectivity:

- Wi-Fi access is provided to staff and student through wireless access points on restricted MAC authentication or secured key to their laptops both in academic and hostels buildings.
- Guest can access Wi-Fi by getting temporary password through IT helpdesk.
- Users have the responsibility to ensure that they are running up to date antivirus software and that the operating system is fully patched with the latest service packs and hot fixes.

## 3. COMPUTER LAB USAGE POLICY

The following guidelines are followed to computer lab to increase the maximum utilizations of the labs:

- Students aren't allowed to disconnect the computers or monitors power supply either from the computer or from the overall purpose outlet. Students are going to be held responsible for any damage caused should they are doing so.
- Students should connect their personal computers to the wired or wireless network points with prior approval from the concern lab technicians.
- Each person entering the computer laboratory must use their ID card to enter the laboratories and other secured spaces.
- No food or drink is to be taken into the computer labs or near any computers.
- Scheduled classes always have priority in computer laboratories as per time table.
- No advertising material is permitted in the laboratories or the surrounding areas unless prior consent has been given in writing by staff.
- Computers are not to be left unattended for more than 15 minutes. Computers that are logged on and left unattended for longer than this time may be logged off without notice and unsaved data will be lost.
- The laboratory computers are provided for research, course work and other sanctioned activity only. Recreational and personal use is not permitted.
- Students are not allowed to install software on to the lab computers under any circumstances, or run any software not installed by technicians.

Director
School of Management Sciences
Lucknow

# 4: IT SECURITY POLICY

The following guidelines are followed to secure the network to avoid un-a authorized access from the outside network

- Indian firewall and IPCOP software base firewall deployed in our campus network to monitor incoming and outgoing network traffic and block unauthorized access from outside.
- IT helpdesk team of our institution should only be allowed to installation and maintenance of servers.

**Deployment Server room equipment's and software's in our campus:**

- Remote access of servers and systems must provide adequate safeguards through robust identification, authentication techniques.

- End users should monitor and ensure installation of antivirus software and its periodical updates in their systems.

- End users should be restricted to installing software and change the configuration of IT equipment's by the user level privileges in their accounts.

- E-mail server and web server should be deployed with security software to scan mail and attachments to prevent viruses.

- Important key areas of our institution will be monitored through CCTV cameras as per surveillance policy of our institution.

# 5. CCTV SURVEILLANCE POLICY

The following procedure is following to monitor the surveillance camera and related equipment's in our institution:

- CCTV Surveillance cameras are fixed in key areas of our institution such as: Gate Entrance and Passages of all blocks, Library, Computer Laboratories, Confidential Sections and Hostels.
- The CCTV will be functioning 24 hours each day with recording facility in DVR.
- The CCTVs are monitored centrally from the institution offices by Administrative Officer and technical staff.
- Adequate signage will be displayed at each area in which CCTV camera is sited to indicate that CCTV is in operation.

The failures of CCTV and its accessories will be rectified on-time and will be taken care by technical team.

- Recorded data will not be retained for longer period if it is not necessary.
- Proper approval should get from the administrative office to view the playback of
- CCTV footages if anyone request.

Director
School of Management Sciences
Lucknow

# 6: BACKUP AND DATA RECOVERY POLICY

The following procedures are followed to back up the data and server from the end user systems:

- Backups will be stored onto internal, external hard disk and in the cloud storage applications.
- Keep and ensure availability of storage media and space for backup in on-site and off-site.
- IT helpdesk · team is responsible to contact the vendor when necessary for troubleshooting for severe issues.
- Backup software used to manage the data backups and recovery process.

The following scheduled process is monitored by technical staff for the backup and retention frequency:

1: Daily Backups

2: Monthly Backups

3: Annual Backups

**Backup Restoration Procedure:**

Users who need file restoration must submit a request to IT helpdesk through online with proper channel. They will need to mention information about the file creation date, name of the file and the last time when it was changed.

# 7: INTERNET AND E-MAIL ACCESS POLICY

The following procedure will be followed to provide Internet access to all the users of the institutions.

- Internet access is provided to all employees and students to all blocks of the institution including hostels with wired and wireless mode of distribution through secured MAC AUTHENTICATION POLICY.
- Content filtering technique has configured on institution firewall to restrict to visit unwanted websites such as: games, online chats, online shopping, pornography, social networks.
- Students and staff can access the Internet without any browsing cost. Internet access by staff and student's activities will be monitored through firewall.
- Internet will be used by staff and students for their academic and administrative related activities of the institution.
- Sharing confidential documents and proprietary information outside of the Institution is strictly prohibited.

Director
School of Management Sciences
Lucknow

The following procedure will be followed to provide E-mail access to all the users of the institutions

- Official Email ID is provided through System admin SMS Lucknow to communicate official information inside and outside the campus.
- Staff must be aware of the potential for on-line personal safety issues on the Internet and Email and ensure that students are supervised during on-line activities.
- Website coordinator has to monitor the official email distribution wherever possible circumstances to maintain authenticity of email access.
- Staff and all users are accountable for e-mail they create and distribute through the network.
- Faculty and Staff must respect the privacy of others. Email should not be forwarded without the express permission of the writer contained with the details provided within the signature block of the original author.
- Users are informed about Virus links send as e-mail attachments. No e-mail has to be clicked or open without checking the sender.

## 8: IT ASSET MANAGEMENT POLICY

The following procedure will be followed for IT asset inventory management in our institution:

Purchase Order

- Authorized staff will raise the purchase indent to the management based on the requirements with detailed configuration. After the approval of purchase indent by the management, purchase department will get the quotations from multiple vendors.
- Validity of quotation should be verified by concern person. Negotiation process is to be finished to get the final price to raise the purchase order by the purchase department in front of the management representatives and vendors.
- After completion of negotiation, purchase committee has to identify which vendor is eligible to get purchase order. Eligible vendor will get purchase order from the purchase manager.

**Responsibilities of Vendor**

- Keep and ensure sufficient date of delivery of IT assets and payment procedure as mentioned on the purchase order.
- At the time of delivery of products, vendor should submit the delivery challan or invoice to the institution with seal and signature.
- Mostly new IT assets should be installed by vendors through authorized technical experts at first time to ensure there is no physical damage in their products and produce installation and warranty reports.

**IT Asset Movement**

- IT assets will be moved to one location to another location based on needs by their IT helpdesk team after approval from the administrative office.
- All movements have entered into concern stock register for tracking assets easily.

Director
School of Management Sciences
Lucknow

**IT Asset Stock Verification**

- Stock verification will be followed for all IT assets at end of the academic year from the stock verification team which is constituted by the institution.
- After the completion of stock verification, the team will submit detailed report to the management.

**Disposal of IT Assets**

- When IT assets have reached the end of their life, IT helpdesk will scrap and e-waste the same.

## 9: PREVENTIVE AND CORRECTIVE ACTION MAINTENANCE POLICY

The following procedures are followed for maintenance of computer lab in the institution:

- Analyze the tasks or jobs required to maintain each piece of equipment as well as the frequency period with which these tasks should performed (i.e. daily, monthly, quarterly, and annually). Preventive maintenance scheduled task is best suited to be in around run-time hours.
- Important equipment's such as server, desktop and CCTV having separate preventive maintenance schedule and checklist are available to increase the equipment performance and reduce the breakdown.
- Information Technology Services reserves the right to perform routine network, desktop and server maintenance and updates after the working hours of institution. Access to ICT enabled services and systems may be down for during this time.
- In-house technicians will take care of entire ICT related equipment at time of preventive and corrective action schedule.
- All the online UPS are under an annual maintenance contract for preventive and corrective action related trouble calls.
- Service request or purchase request will be raised to management if there is any major failure occurred in the equipment or parts of equipment.

## 10: SERVER MAINTENANCE POLICY

The following procedures are followed to maintain server to increase the performance and speed of the operations.

- Server configuration details including security measures and details of privileges accounts are maintained by computer cell.
- All servers should be dedicated to the specific tasks associated with its role and located in a protected area with restricted-access from end users.
- Database backups are periodically taken and retained specific locations as per backup and

Director
School of Management Sciences
Lucknow

restoration policy.

- Install new updates and security patches are very important to keep server hardware and software up-to-date.
- Review the username and password at specific interval and change the password periodical time and ensure complexity of password creation procedure.
- Before making any changes to server should ensure backups are working properly. You may run few test recoveries if you are going to erase critical data and codlings.

## 11: SOFTWARE INSTALLATION AND LICENSING POLICY

The following guidelines are followed to install software and monitor the piracy frees software's inside the campus.

- All software installed in computers and network devices shall be appropriately licensed by the institution.
- System requirements should be checked by IT helpdesk before installing any software's to maintain performance of computing devices.
- The IT helpdesk team will install application software's requested by the staff as pert he guidelines of the policy and licensing manual.
- Institution shall maintain sufficient documentation to validate that the software is appropriately licensed.
- All the Academic I Non-Academic staff shall accept the responsibility to prevent illegal software usage and abide by the policy.
- Distributing or sharing of software to unauthorized person is highly prohibited.
- Software Applications or Packages will be installed in all computer laboratories based on request from heads of departments with prior approval from the head of the institution for the academic semester as per the curriculum.
- Periodical Updates of Software is more essential as they come across critical patches, bugs troubleshoot upon update as well it will overcome the security holes which will bring improve the performance of the computer.
    - The institution shall audit periodical time to ensure piracy free software's installed in the computer systems.