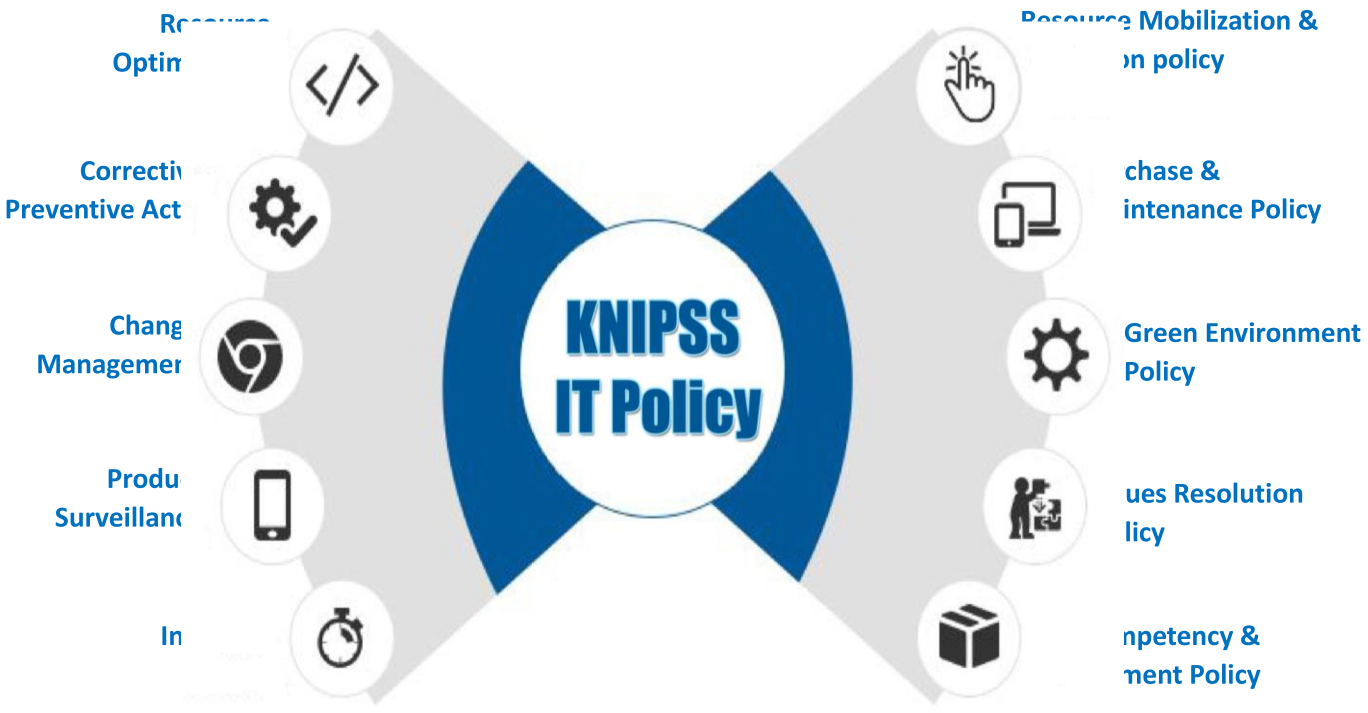
KAMLA NEHRU INSTITUTE OF PHYSICAL AND SOCIAL SCIENCES

(Affiliated to Dr. Ram Manohar Lohia Avadh University Ayodhya U.P.)

Accredited by NAAC with 'A' Grade (2nd Cycle),

An ISO 9001:2015 Certified Institution Sultanpur-228 118, Uttar Pradesh, India

IT Policy



KNIPSS

SULTANPUR | U.P. | INDIA

IT POLICY

1. USER ACCOUNT AND PASSWORD MANAGEMENT POLICY

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

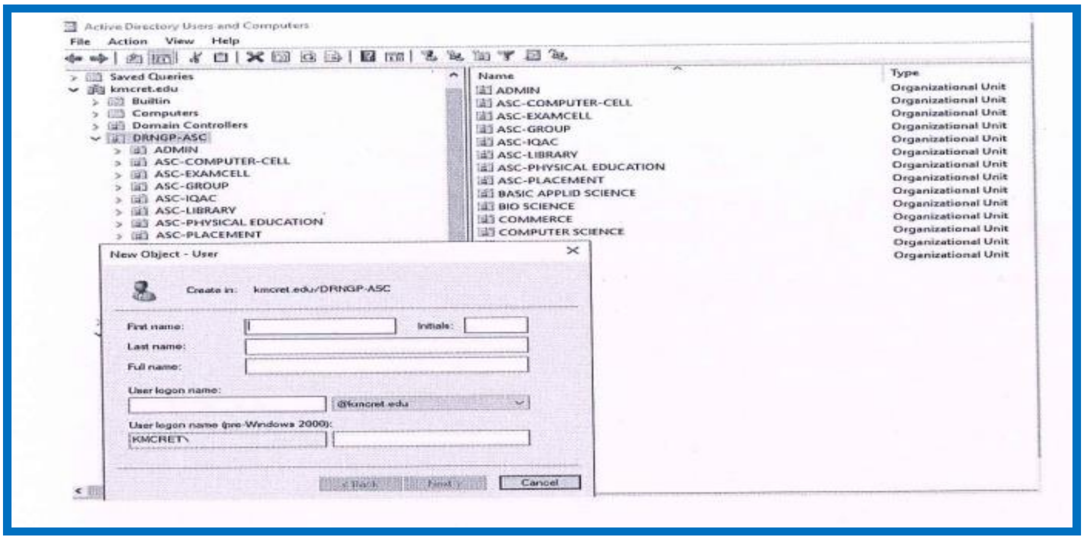
- Register number will be the user's name for all students to access the computers in computer labs which is created in server.
- Students must change their default password which IS received from concern lab technicians at the time of their first login.
- Students having user name and password with limited privileges to prevent the configuration changes of network systems.
- Student should disable remember user name and password option in their systems during login time.
- 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 have forgotten password or security breach happens.
- Students should not share their email passwords or system 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.
- Employee id will be the user's name for staff to access the Internet in our institution. Default password will be provided at the time of first login by the helpdesk of IT team. Staff can change their password during the first login attempt.
- Sharing folder in server can be access by the authorized staff members through separate user name and password 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 in easy access areas,
- Passwords should not contain the first name of staff or equipment.



- Saved Queries
- kmcret.edu
  - Builtin
  - Computers
  - Domain Controllers
  - DRNGP-ASC
    - ADMIN
    - ASC-COMPUTER-CELL
    - ASC-EXAMCELL
    - ASC-GROUP
    - ASC-IQAC
    - ASC-LIBRARY
    - ASC-PHYSICAL EDUCATION
    - ASC-PLACEMENT

Name	Type
ADMIN	Organizational Unit
ASC-COMPUTER-CELL	Organizational Unit
ASC-EXAMCELL	Organizational Unit
ASC-GROUP	Organizational Unit
ASC-IQAC	Organizational Unit
ASC-LIBRARY	Organizational Unit
ASC-PHYSICAL EDUCATION	Organizational Unit
ASC-PLACEMENT	Organizational Unit
BASIC APPLID SCIENCE	Organizational Unit
BIO SCIENCE	Organizational Unit
COMMERCE	Organizational Unit
COMPUTER SCIENCE	Organizational Unit
	Organizational Unit
	Organizational Unit

New Object - User

Create in: kmcret.edu/DRNGP-ASC

First name: Initials:

Last name:

Full name:

User logon name: @kmcret.edu

User logon name (pre-Windows 2000): KMCRET\

2. WIRED AND WIRLESS NETWORK ACCESS POLICY

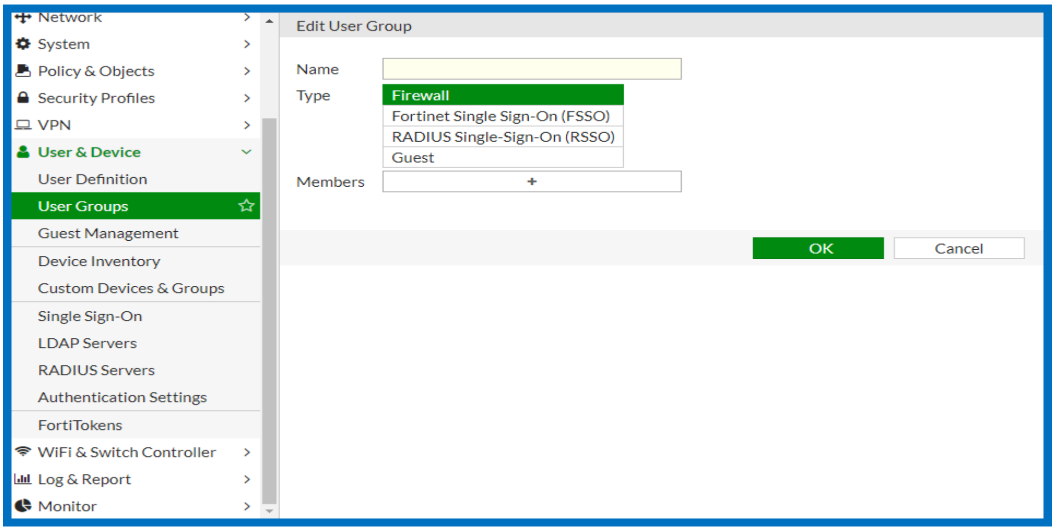
The following guidelines are followed to wired network to enrich the performance and speed of network connectivity:

- Network connectivity provided to all blocks of the Institution in an authenticated network access through firewall and VLAN connectivity.
- Any desktop or server that will be connected to the network is configured with a 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 firewall.

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

- The registration of Wi-Fi access is processed after verification of the technical and personnel details of the user which is filled by them through an online request form in our website.

- 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 softwareand that the operating system is fully patched with the latest service packs and hot fixes.



Edit User Group

Name

Type: Firewall

Fortinet Single Sign-On (FSSO)

RADIUS Single-Sign-On (RSSO)

Guest

Members +

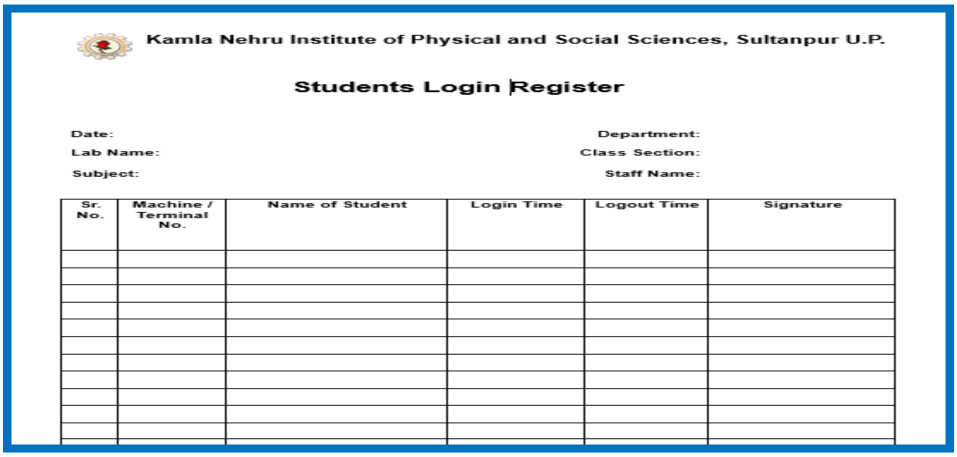
3. COMPUTER LAB USAGE POLICY

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

- Students aren’t 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 laboratoriesarid 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.
- Print quota is for the printing of experiments only. Lecture notes and

other materials are provided in classes and are not to be printed in the labs.

- 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 to install software on to the lab computers under any circumstances,or run any software not installed by technicians.



Kamla Nehru Institute of Physical and Social Sciences, Sultanpur U.P.

Students Login Register

Date: Department:
Lab Name: Class Section:
Subject: Staff Name:

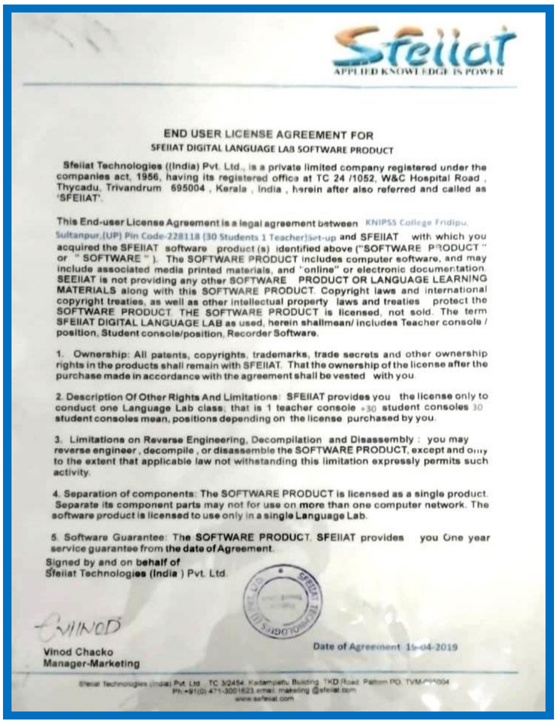
Sr. No.	Machine / Terminal No.	Name of Student	Login Time	Logout Time	Signature

4. SOFTWARE INSTALLATION AND LICENSING POLICY

The following guidelines are followed to install software and monitor the piracy Free 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'sto maintain performance of computing devices.
- The IT helpdesk team will install application software's requested by the staff as per the guidelines of the policy and licensing manual.
- Institution shall maintain sufficient documentation to validate that the softwareis appropriately licensed.
- All the Academic / 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.
- Make sure un-used software packages not covering the curriculum and no longer used shall be uninstalled.



Sfeiiat
APPLIED KNOWLEDGE IS POWER

END USER LICENSE AGREEMENT FOR
SFEIIAT DIGITAL LANGUAGE LAB SOFTWARE PRODUCT

Sfeiiat Technologies ((India) Pvt. Ltd., is a private limited company registered under the companies act, 1956, having its registered office at TC 24 /1052, W&C Hospital Road , Thycadu, Trivandrum 695004 , Kerala , India , herein after also referred and called as 'SFEIIAT'.

This End-user License Agreement is a legal agreement between KNIPSS College Fridipu, Sultanpur,(UP) Pin Code-228118 (30 Students 1 Teacher)Set-up and SFEIIAT with which you acquired the SFEIIAT software product (s) identified above ("SOFTWARE PRODUCT" or " SOFTWARE "). The SOFTWARE PRODUCT includes computer software, and may include associated media printed materials, and "online" or electronic documentation. SEEIIAT is not providing any other SOFTWARE PRODUCT OR LANGUAGE LEARNING MATERIALS along with this SOFTWARE PRODUCT. Copyright laws and international copyright treaties, as well as other intellectual property laws and treaties protect the SOFTWARE PRODUCT. THE SOFTWARE PRODUCT is licensed, not sold. The term SFEIIAT DIGITAL LANGUAGE LAB as used, herein shallmean/ includes Teacher console / position, Student console/position, Recorder Software.

1. Ownership: All patents, copyrights, trademarks, trade secrets and other ownership rights in the products shall remain with SFEIIAT. That the ownership of the license after the purchase made in accordance with the agreement shall be vested with you.

2. Description Of Other Rights And Limitations: SFEIIAT provides you the license only to conduct one Language Lab class; that is 1 teacher console +30 student consoles 30 student consoles mean, positions depending on the license purchased by you.

3. Limitations on Reverse Engineering, Decompilation and Disassembly : you may reverse engineer , decompile , or disassemble the SOFTWARE PRODUCT, except and only to the extent that applicable law not withstanding this limitation expressly permits such activity.

4. Separation of components: The SOFTWARE PRODUCT is licensed as a single product. Separate its component parts may not for use on more than one computer network. The software product is licensed to use only in a single Language Lab.

5. Software Guarantee: The SOFTWARE PRODUCT, SFEIIAT provides you One year service guarantee from the date of Agreement.

Signed by and on behalf of
Sfeiiat Technologies (India) Pvt. Ltd

SFEIIAT TECHNOLOGIES (I) PVT. LTD.

VINOD
Vinod Chacko
Manager-Marketing

Date of Agreement 15-04-2019

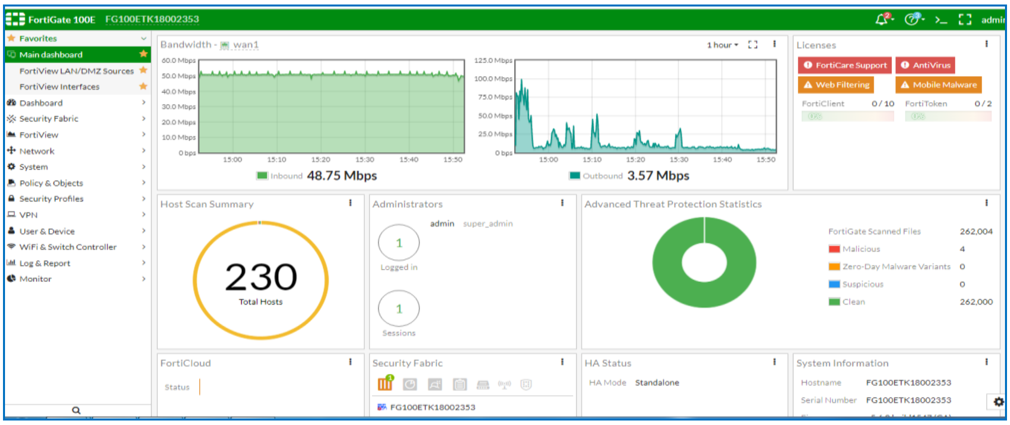
Sfeiiat Technologies (India) Pvt. Ltd. TC 3/2454, Kadampattu Building, TKD Road, Pattom PO, TVM-[illegible]004
Ph:+91(0) 471-3001623 email: marketing @sfeiiat.com
www.sfeiiat.com

5. IT SECURITY POLICY

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

- Firewall is a network security device that 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 deployment of IT equipment's and software's in our campus.

- Access to systems and their data must be restricted to ensure that information is denied to unauthorized users. All the IT equipment’s of our institutions will be accessed through authorized username and password only,
- Enterprise security antivirus software is installed in all computers to prevent malwares, worms, viruses spread into network.
- 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 configurationof 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.
- Backup of database and files will be stored and retained in on-site and off-site of campus for emergency and disaster period as per backup and restoration policy of our institution.



Inbound 48.75 Mbps

Outbound 3.57 Mbps

FortiClient 0 / 10 FortiToken 0 / 2

230 Total Hosts

admin super_admin

1 Logged in

1 Sessions

FortiGate Scanned Files	262,004
🟥 Malicious	4
🟧 Zero-Day Malware Variants	0
🟦 Suspicious	0
🟩 Clean	262,000

Status

FG100ETK18002353

HA Mode Standalone

Hostname FG100ETK18002353

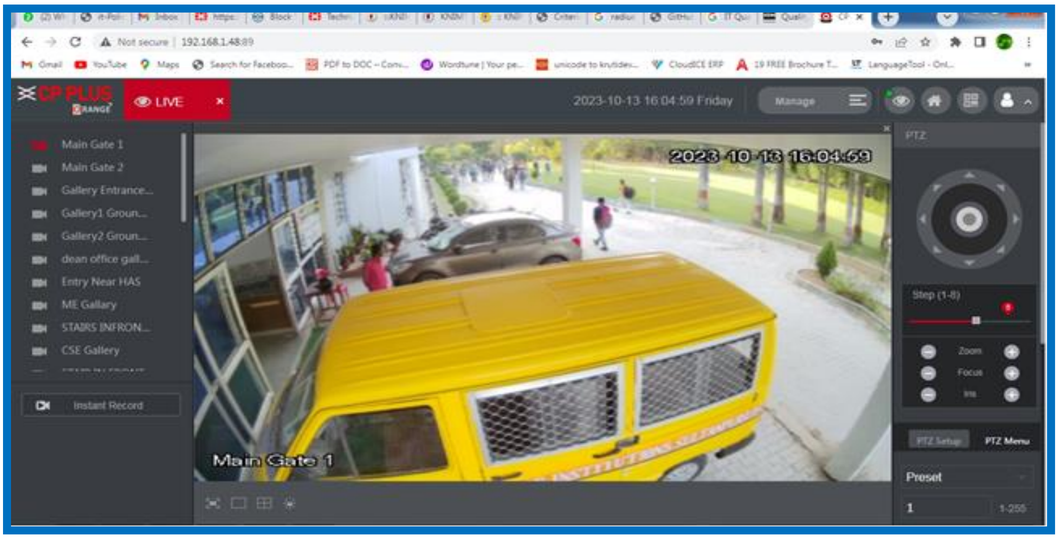
Serial Number FG100ETK18002353

6. 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 except live audio/sound.
- The CCTV s 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.
- Footages of CCTV s are recorded through NVRJDVRs and stored in an internal hard disk drive.
- Storage of recordings will be kept for 30 days; at the end of 30 days the storage media will be over righting with new recordings.
- 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.



7. BACKUP AND DATA RECOVERY POLICY

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

- An automated scheduled incremental backup method is availed daily in our institution which successive copies of the data contain only the portion that has changed since the preceding backup copy was made.

- To ensure backed up data is stored in an on-site and off-site location and can be easily found and recovered in the event of any equipment failure, intentional destruction of data, or disaster.
- Backups will he stormed onto internal, external hard disk and in the cloud storage applications.
- Checking backup software log reports to ensure that tasks were completed without errors.
- 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 trouble shooting 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:

Daily Backups

- Incremental backups will be stored in external storage media for the period of one month.
- Backup schedule will be created in server once per hour in confidential areas.
- Backup schedule will be created in server twice per day in other than confidentialareas.

Monthly Backups

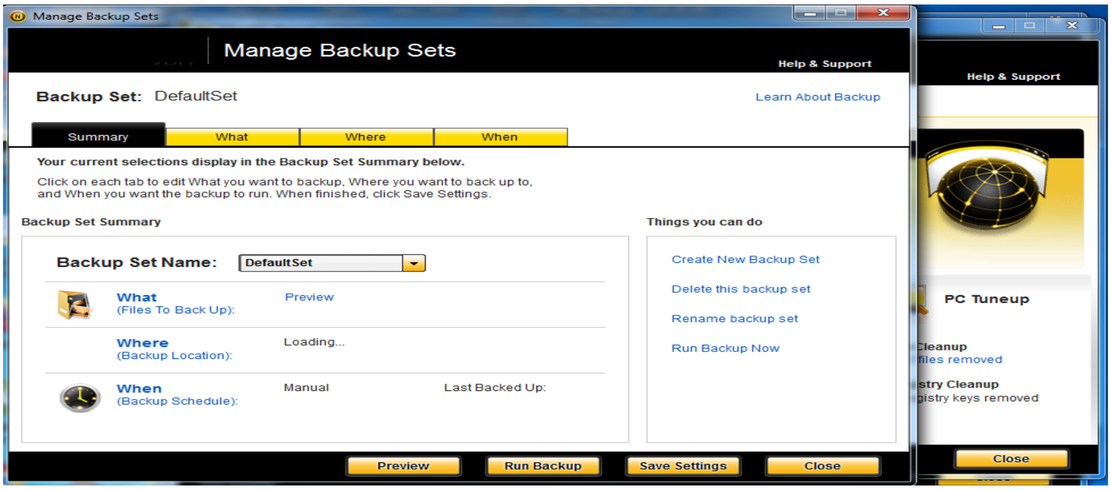
- Full backups will be stored and retained in on-site and off-site for three months.
- Packing monthly backups storage media and send it to off-site for retention.

Annual Backups

- Full backups of confidential sections will be stored and retained in on-site and off-site for three years.
- Storage media will be reused after three years if that are still viable.

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.



Manage Backup Sets

Backup Set: DefaultSet

Your current selections display in the Backup Set Summary below.

Click on each tab to edit What you want to backup, Where you want to back up to, and When you want the backup to run. When finished, click Save Settings.

Backup Set Summary

Backup Set Name: DefaultSet

What (Files To Back Up): Preview

Where (Backup Location): Loading...

When (Backup Schedule): Manual Last Backed Up:

Things you can do

- Create New Backup Set
- Delete this backup set
- Rename backup set
- Run Backup Now

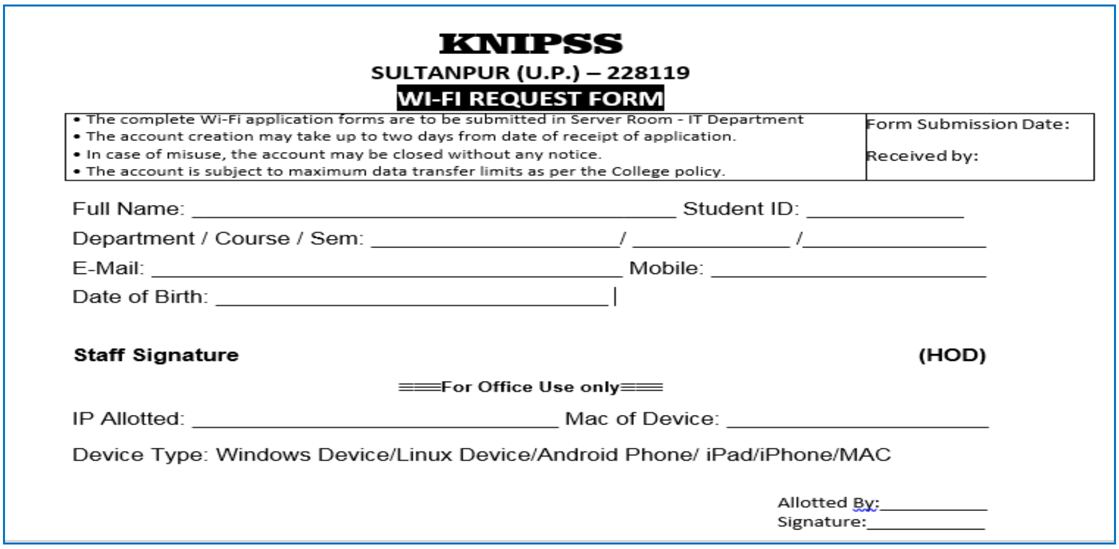
PC Tuneup

8. ICT ENABLED CLASS ROOM POLICY

The following procedure will be followed to establish and monitor the ICT enabled classrooms to the entire campus:

- ICT has a promise to improve the quality of teaching and learning process. Moderntechnology like electronics and telecommunication provide to strengthen the voice of lecture.
- ICT helps students to explore knowledge to learn the content through self-study. Access of course materials through remote devices from servers. Online digital repositories for lectures, course materials, and digital library.
- Teacher can help the students by ensuring the right direction towards effective learning. Situational learning, programmed learning, many Online learning courses are some of the example of self-learning strategies that are being utilized with the help of ICT.
- All class rooms have been equipped with projector to enhance the teaching learning process. Wireless and Wired Local Area Connection facilities are equipped in all classes to access Internet and Intranet applications to the students.
- There are other tools such as headphones, video cameras, and webcams,

audio recordingsoftware that also encourage the development of speaking and listening skills based on needs.



KNIPSS

SULTANPUR (U.P.) – 228119

WI-FI REQUEST FORM

• The complete Wi-Fi application forms are to be submitted in Server Room - IT Department • The account creation may take up to two days from date of receipt of application. • In case of misuse, the account may be closed without any notice. • The account is subject to maximum data transfer limits as per the College policy.	Form Submission Date: Received by:

Full Name: ____ Student ID: __________

Department / Course / Sem: ____________________/ ___________ /_____________

E-Mail: _______________________________________ Mobile: _____________________

Date of Birth: ________________________________|

Staff Signature **(HOD)**

≡≡≡For Office Use only≡≡≡

IP Allotted: ______________________________ Mac of Device: _____________________

Device Type: Windows Device/Linux Device/Android Phone/ iPad/iPhone/MAC

Allotted By:__________
Signature:__________

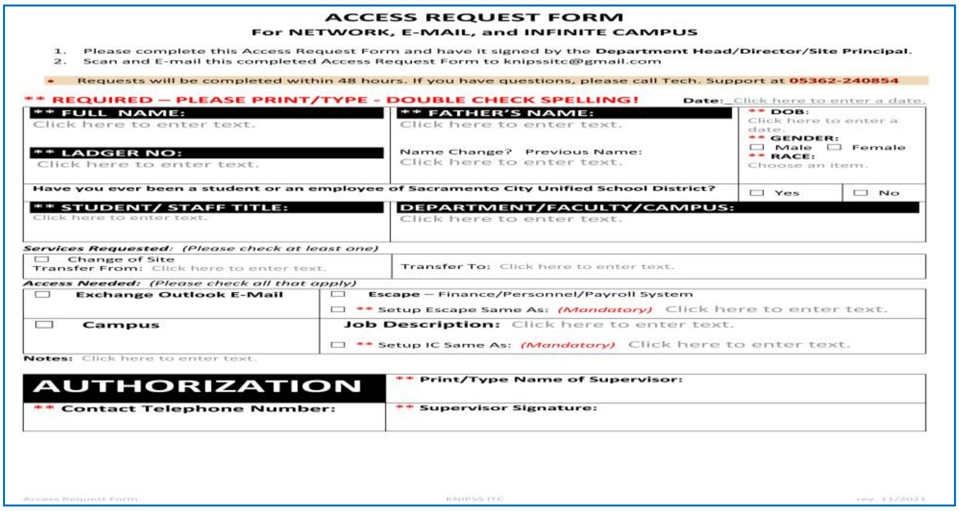
9. INTERNET AND E-MAIL ACCESS POLICY

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 institutionincluding hostels with wired and wireless mode of distribution through secured firewall connectivity.
- All staff should get user credentials from IT helpdesk to access the Internet inside the institution. Employee ID will be the username for internet access. Default password should be changed by the employee at the time of first login itself.
- Content filtering technique has configured in institution firewall to restrict to visitunwanted 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.

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

- Staff should identify themselves properly when using Email through the use of a signature block at the conclusion of e-mail messages The signature block will state the employee's name, position, and include a disclaimer stating that the Email is intended only for the nominated recipient and if received in error the sender should be notified as soon as possible.
- Official Email ID is provided through website coordinator 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 must 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.
- Staff and students must respect the privacy of others. Email should not be forwardedwithout the express permission of the writer contained with the details provided within the signature block of the original author.
- Virus protection programs are to be set to automatically scan email on download,and all downloaded files on first use. Files downloaded from the Internetare to be saved to disk first, and then scanned before being opened / installed.



ACCESS REQUEST FORM

For NETWORK, E-MAIL, and INFINITE CAMPUS

1. Please complete this Access Request Form and have it signed by the **Department Head/Director/Site Principal**.
2. Scan and E-mail this completed Access Request Form to knipssitc@gmail.com

- Requests will be completed within 48 hours. If you have questions, please call Tech. Support at 05362-240854

** REQUIRED – PLEASE PRINT/TYPE - DOUBLE CHECK SPELLING! Date: Click here to enter a date.

** FULL NAME: Click here to enter text. ** LADGER NO: Click here to enter text.	** FATHER'S NAME: Click here to enter text. Name Change? Previous Name: Click here to enter text.	** DOB: Click here to enter a date. ** GENDER: □ Male □ Female ** RACE: Choose an item.
Have you ever been a student or an employee of Sacramento City Unified School District?	□ Yes	□ No
** STUDENT/ STAFF TITLE: Click here to enter text.	DEPARTMENT/FACULTY/CAMPUS: Click here to enter text.	

Services Requested: (Please check at least one)

□ Change of Site Transfer From: Click here to enter text.	Transfer To: Click here to enter text.

Access Needed: (Please check all that apply)

□ Exchange Outlook E-Mail	□ Escape – Finance/Personnel/Payroll System □ ** Setup Escape Same As: *(Mandatory)* Click here to enter text.
□ Campus	Job Description: Click here to enter text. □ ** Setup IC Same As: *(Mandatory)* Click here to enter text.

Notes: Click here to enter text.

AUTHORIZATION	** Print/Type Name of Supervisor:
** Contact Telephone Number:	** Supervisor Signature:

Access Request Form KNIPSS ITC rev. 11/2021

10. IT ASSET MANANGEMENT POLICY

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

Purchase Indent

- 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 mentionedon 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 technicalexperts at first time to ensure there is no physical damage in their products and produce installation and warranty reports.

IT Asset Movement

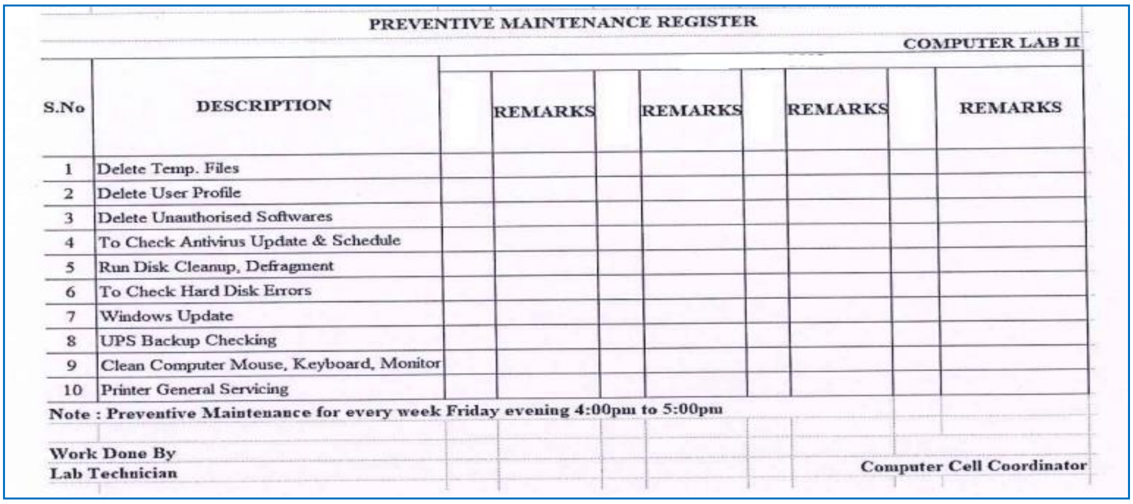
- IT assets will be moved to one location to another location based on needs by the IT helpdesk team after approval from the administrative office.
- All movements have entered into concern stock register and online web portal for tracking assets easily.

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 dispatch the equipment as e-waste through proper manner.
- IT help desk will follow the guidelines for disposal of IT assets based on e-waste management policy.
- All the data and configurations of IT assets will be deleted before disposal of e-waste.



PREVENTIVE MAINTENANCE REGISTER

COMPUTER LAB II

S.No	DESCRIPTION		REMARKS		REMARKS		REMARKS		REMARKS
1	Delete Temp. Files								
2	Delete User Profile								
3	Delete Unauthorised Softwares								
4	To Check Antivirus Update & Schedule								
5	Run Disk Cleanup, Defragment								
6	To Check Hard Disk Errors								
7	Windows Update								
8	UPS Backup Checking								
9	Clean Computer Mouse, Keyboard, Monitor								
10	Printer General Servicing								

Note : Preventive Maintenance for every week Friday evening 4:00pm to 5:00pm

Work Done By
Lab Technician

Computer Cell Coordinator

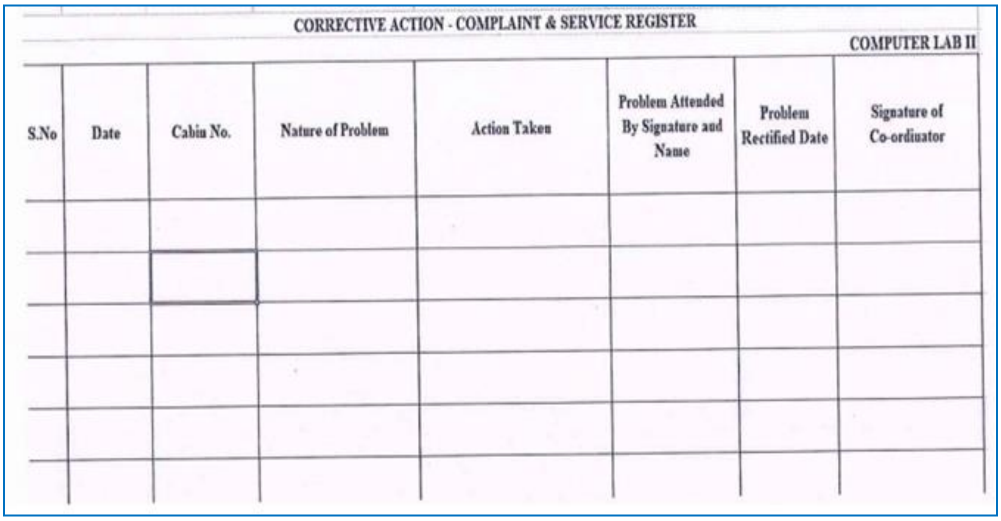
11. PREVENTIVE AND CORRECTIVE ACTION MAINTENANCE POLICY

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 preventivemaintenance schedule and checklist are available to increase the equipment performance and reduce the breakdown.
- Information Technology Services reserves the right to perform routine network, desktopand 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.



CORRECTIVE ACTION - COMPLAINT & SERVICE REGISTER

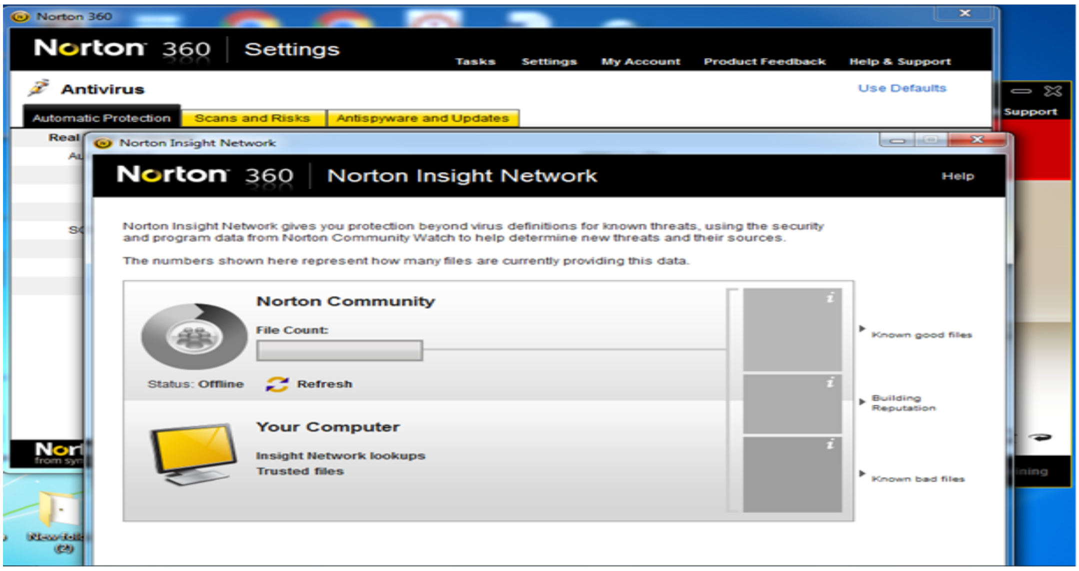
COMPUTER LAB II

S.No	Date	Cabin No.	Nature of Problem	Action Taken	Problem Attended By Signature and Name	Problem Rectified Date	Signature of Co-ordinator

12. PRINTING / SCANNING / REPROGRAPHY POLICY

The following procedures are followed for printing by staff and students for record note and other academic related activities.

- Reprographic section is available inside the campus for Staff and Students to avail the services.
- All should practice all reasonable steps to reduce the usage of printers, copiers and consumables.
- Students can take prints for their record notes in computer laboratories those who are having computer practical.
- All charges for student printing will be managed by IT Services and utilized to manageand provide equipment, servicing, consumables and other associated costs and to develop service improvements. Charges to students will be subject to the total cost of providing the service.
- Staff wants to print large or multiple documents (eg, booklets) should utilize college commercial printing services rather than local small printers.
- Student and staff can avail the scanning, services in Reprography section to scan the official document without any cost.
- Scanned document can be sent to their e-mail id.



Norton Insight Network gives you protection beyond virus definitions for known threats, using the security and program data from Norton Community Watch to help determine new threats and their sources.

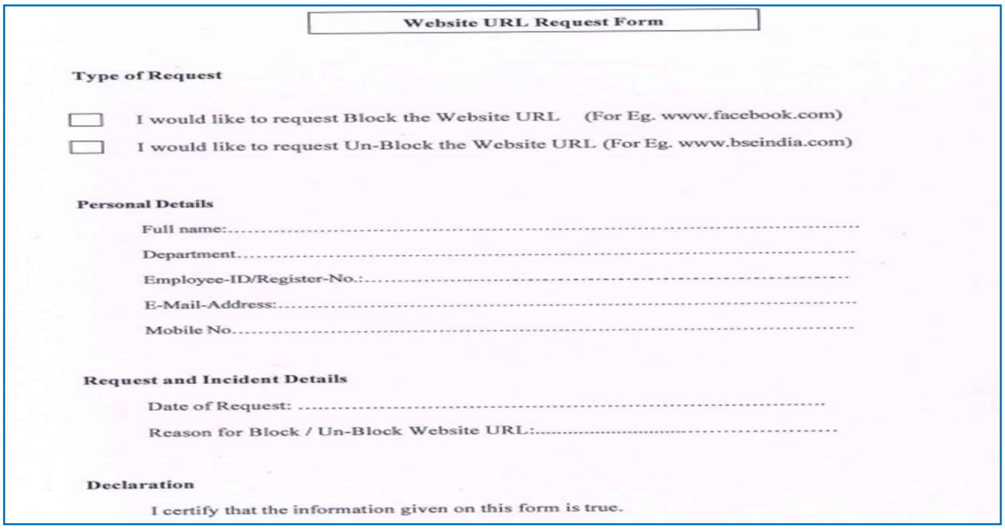
The numbers shown here represent how many files are currently providing this data.

13. 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 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.
- RAID controller must be used in all servers to avoid data loss during disk failure and disaster period of time.
- Regular security audits should be done into all servers to check the system configuration,OS updates and other potential security risks.

- Hard Disk usage and user account role must be checked at specific interval to increase the performance of server.



Website URL Request Form

Type of Request

□ I would like to request Block the Website URL (For Eg. www.facebook.com)

□ I would like to request Un-Block the Website URL (For Eg. www.bseindia.com)

Personal Details

Full name:..

Department..

Employee-ID/Register-No.:..

E-Mail-Address:...

Mobile No...

Request and Incident Details

Date of Request: ....

Reason for Block / Un-Block Website URL:...

Declaration

I certify that the information given on this form is true.

14. WARRANTY AND AMC CONTRACT POLICY

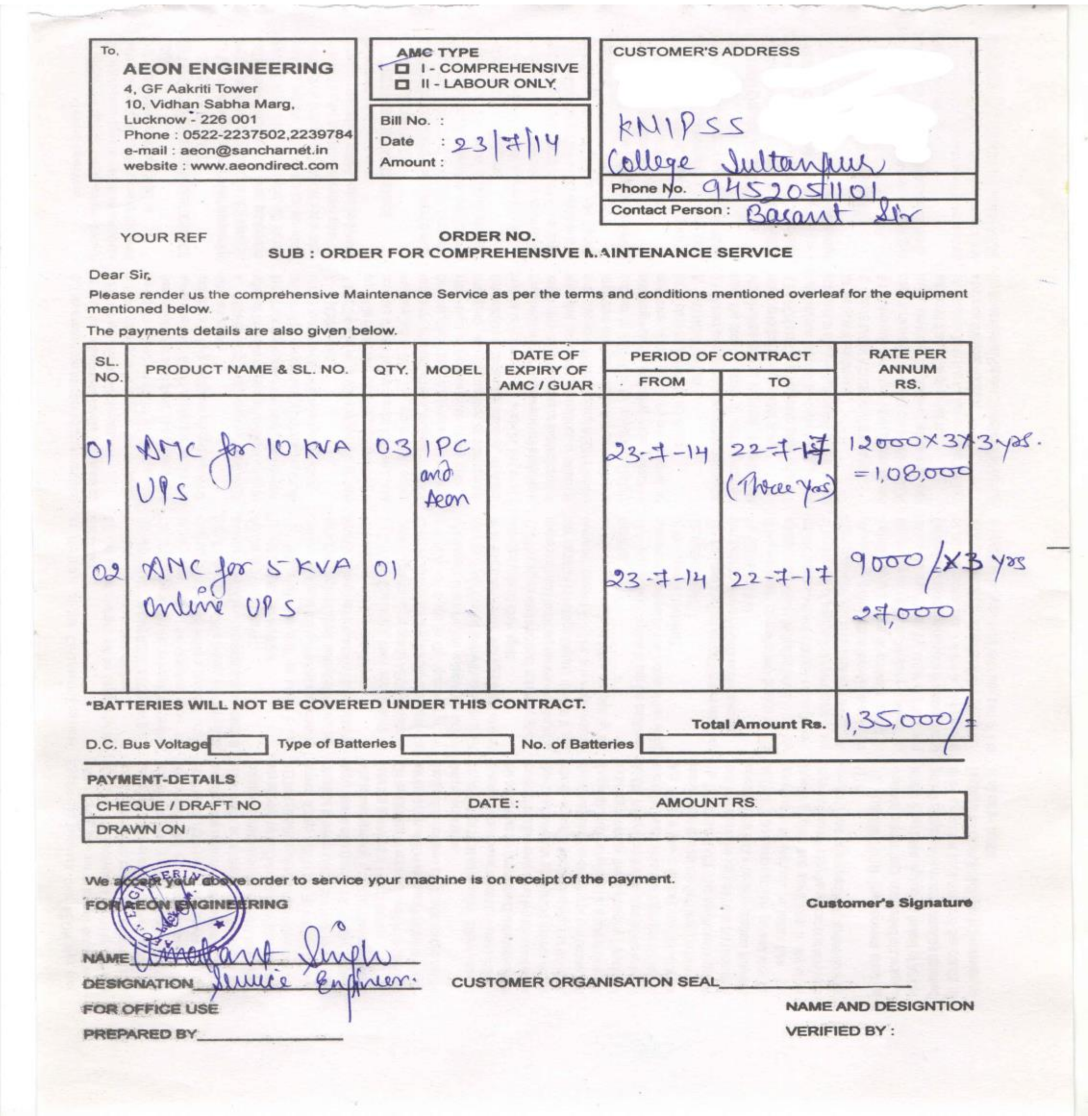
Computers and IT assets purchased by our institution should preferably cover with 3 years on-site comprehensive warranty except few assets from the data of installation. After the expiry of warranty period, IT assets should be under the maintenance of in-house lab technicians of computer lab.

The following are the procedure of warranty claim:

- Complaint request will be given to vendor who 1S supplied the particular equipmentor the manufacturer through online or voice call. They will issue the case id or reference number against the complaint request.
- Based on complaint, technical person will come to on-site to observe the complaint and service or replace the equipment or part of equipment. Sometimes equipmentor part of equipment will be dispatched to service vendor if not able to service at on-site through proper channel.
- After completion of service equipment, in-house technician will verify the equipment status and authorize to raise service report to close the complaint request.

The following are the procedure of AMC claim:

- Service request will be raised by in-house technicians to concern vendor whenever the equipment failure.
- Service engineers will reach on-site to rectify the equipment problem on the day of complaint. In critical case, sensitive electronic boards will be sent to them for chip level service through proper channel.
- After completion of service equipment, in-house technician will verify the equipment status and authorize to raise service report to close the complaint request.
- Preventive maintenance is scheduled once in quarter to enrich the performance of equipment as per annual maintenance contract.
- During preventive maintenance time, inner and outer side of equipment's will be cleaned through air blower by the authorized service engineers,
- Distilled water will be filled to batteries of UPS whenever required to increase the life of battery and enrich the equipment performance.



To,
AEON ENGINEERING
4, GF Aakriti Tower
10, Vidhan Sabha Marg,
Lucknow - 226 001
Phone : 0522-2237502,2239784
e-mail : aeon@sancharnet.in
website : www.aeondirect.com

AMC TYPE
☑ I - COMPREHENSIVE
□ II - LABOUR ONLY

Bill No. :
Date : 23/7/14
Amount :

CUSTOMER'S ADDRESS
KNIPSS
College Sultanpur
Phone No. 9452051101
Contact Person : Basant Sir

YOUR REF

ORDER NO.

SUB : ORDER FOR COMPREHENSIVE MAINTENANCE SERVICE

Dear Sir,

Please render us the comprehensive Maintenance Service as per the terms and conditions mentioned overleaf for the equipment mentioned below.

The payments details are also given below.

SL. NO.	PRODUCT NAME & SL. NO.	QTY.	MODEL	DATE OF EXPIRY OF AMC / GUAR	PERIOD OF CONTRACT		RATE PER ANNUM RS.
					FROM	TO	
01	AMC for 10 KVA UPS	03	IPC and Aeon		23-7-14	22-7-17 (Three Yrs)	12000×3×3 yrs. =1,08,000
02	AMC for 5 KVA online UPS	01			23-7-14	22-7-17	9000/×3 yrs 27,000

*BATTERIES WILL NOT BE COVERED UNDER THIS CONTRACT.

Total Amount Rs. 1,35,000/=

D.C. Bus Voltage □ Type of Batteries □ No. of Batteries □

PAYMENT-DETAILS

CHEQUE / DRAFT NO DATE : AMOUNT RS.
DRAWN ON

We accept your above order to service your machine is on receipt of the payment.

FOR AEON ENGINEERING

AEON ENGINEERING

Customer's Signature

NAME Umakant Singh
DESIGNATION Service Engineer.

CUSTOMER ORGANISATION SEAL________

FOR OFFICE USE

NAME AND DESIGNTION

PREPARED BY________

VERIFIED BY :

CCTV Footage Request Form

Type of Request :

- I would like to view CCTV footage.
- I would like to request a copy of CCTV footage.

Personal Details :………………………………………………….

Full name:………………………………………………….

Department :………………………………………………….

Employee- ID/Register-No. :………………………………………………….

E-Mail-Address:………………………………………………….

Mobile No :………………………………………………….

Request and Incident Details

Date of Request:	
Date of Incident:	
Time Period of Incident:	

Description of Incident with location:

Declaration

I certify that the information given on this form is true.

Signature of Applicant

15. E-WASTE DISPOSAL POLICY

Institution has formed waste management committee to monitor the e-waste things are disposed in proper manner. Also, we provide orientation to our students and staff how to dispose the e-waste in systematic manner through pollution control departments and agencies.

There are three key principles are followed to disposal of un-used or out dated electrical and electronics appliances in our Institution to manage e-waste management.

- Donated low configuration desktops to nearby government schools,
- Return to Manufacturer for re-cycle.
- Dispose as scrap through vendors.