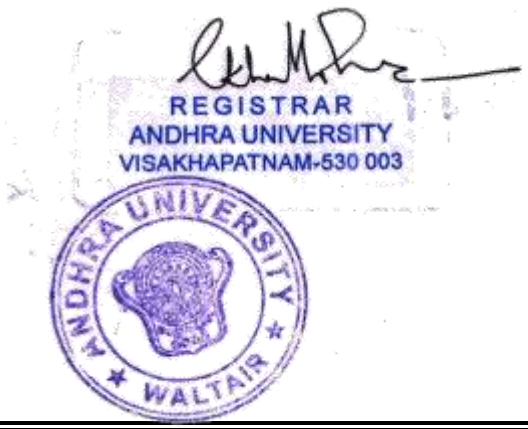
ANDHRA UNIVERSITY

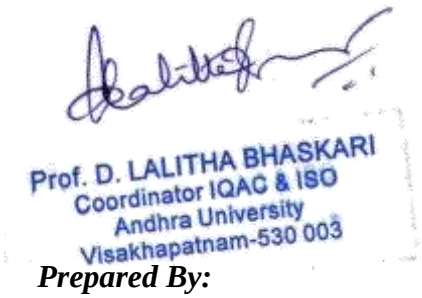
ఆంధ్ర విశ్వకళా పరిషత్

Accredited by NAAC with 'A' Grade ISO 9001: 2015 Certified

Information Technology Policy and Procedure Manual

Policy Number: AU/ITPP/V1.0
Policy Date: 05/09/2019





Prepared By:
The Coordinator
Internal Quality Assurance Cell
ANDHRA UNIVERSITY

Table of Contents

			Page No.
1.	**Introduction**	**:**	**1**
1.1	Purpose of the Policy	:	1
2	**Procedures for IT Hardware Purchase & Software Installation Policy**	**:**	**2**
2.1	Purchase of Hardware	:	2
2.1.1	Request for Hardware	:	2
2.1.2.	Purchase of Hardware	:	2
2.2	Policy for Purchasing/Installation of Software	:	3
2.2.1	Request for Software	:	3
2.2.2	Purchase of Software	:	3
2.2.3	Obtaining open source or freeware software	:	4
2.2.4	Software Licensing	:	4
2.2.5	Software Installation	:	4
2.2.6	Software Usage	:	5
2.3	Policy for Identifying USERS and their responsibilities:		5
2.4	Bring Your Own Device Policy	:	9
2.4.1	Registration of personal mobile devices for institution use:		9
2.4.2	Breach of this policy	:	11
2.4.3	Indemnity	:	11
3.	**Information Technology Security Policy**	**:**	**12**
3.1	Physical Security	:	12
3.2	Information Security	:	13
3.3	Technology Access	:	13
4.	**Information Technology Administration Policy**	**:**	**14**
4.1	Website Policy	:	15

	4.2	Website Register	:	15
	4.3	Website Content	:	16
5.	**Electronic Transactions Policy**		**:**	**16**
	5.1	Electronic Funds Transfer (EFT)	:	17
	5.2	Electronic Purchases	:	18
	5.3	IT Service Agreements Policy	:	18
6.	**Emergency Management of Information Technology**		**:**	**19**
	6.1	IT Hardware Failure	:	20
	6.2	Point of Sale Disruptions	:	20
	6.3	Virus or other security breach	:	20
	6.4	Website Disruption	:	21
7.	**Video Surveillance Policy**	-	**:**	**21**
	7.1	The Security Control Room	:	22
	7.2	AU Security Control Room Administration and Procedures:		23
	7.3	AU Security Control Room Staff	:	24
	7.4	Recording	:	24
	7.5	Access to images	:	24
	7.6	Complaints	:	25
		Appendix - I	:	27

1. Introduction

The Andhra University Information Technology (IT) Policy and Procedure Manual provides the policies and procedures for selection and use of IT within the institution which must be followed by all staff. It also provides guidelines Andhra University will use to administer these policies, with the correct procedure to follow which are applicable to all the employees.

Andhra University will keep all IT policies current and relevant. Therefore, from time to time it will be necessary to modify and amend some sections of the policies and procedures, or to add new procedures. Hence any suggestions, recommendations or feedback on the policies and procedures specified in this manual are welcome.

1.1 Purpose of the Policy

This policy provides guidelines for the purchase of hardware for the institution to ensure that all hardware technology for the institution is appropriate, value for money and where applicable integrates with other technology for the institution. The objective of this policy is to ensure that there is minimum diversity of hardware within the institution. This policy establishes University-wide strategies and responsibilities for protecting the Confidentiality, Integrity, and Availability of the information assets which include data, computers, information systems, network devices, intellectual property and other important documents that are accessed, created, managed, and/or controlled by the University.

2. Procedures for IT Hardware Purchase &Software Installation Policy

2.1 Purchase of Hardware

Policy number: AU/ITPP/P1/V1.0

Few Terms: Computer hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, battery, SMPS and RAM. System refers to Desktops/Laptops/Workstations/Servers/Tablets.

External hardware devices include monitors, keyboards, mice, printers,USB,network cables, network switches, cables,scanners, tablets, UPS, biometric devices, CC cameras, CC TV's and any device related to Internal or external hardware.

Procedure:

2.1.1 Request for hardware: The requirement of hardware by the user department is requisitioned along with specification and estimate submitted for administrative sanction to procure competitive quotations from difference suppliers for approval from Central Purchase Committee (CPC) prior to the use, purchase or installation of any such hardware.

2.1.2 Purchase of hardware:

The purchase of any hardware item like mentioned above should include the relevant components depending upon the hardware. Since hardware needs to be upgraded as and when required any change from the already purchased hardware or new hardware above must be authorized by Central Purchase Committee (CPC) or any competent authority of the university.

All the purchases of any hardware must be supported by appropriate quotations from three vendors including all the required specifications, warranty requirements and GST.

All purchases for any hardware must be in line with the purchasing policy of the University. The purchase of all desktops, servers, portable computers, computer peripherals, mobile devices, Wi-Fi devices, CCTV's, Biometric devices and hence any device which suits the hardware specifications which is to be purchased must adhere to this policy.

2.2 Policy for Purchasing/Installation of Software

Policy number: AU/ITPP/P2/V1.0

Procedures:

2.2.1 Request for Software:

All software, including windows, Linux, Mac and any type of Open source software, licensed versions must be approved by Director, Computer Center/Registrar/Head of the department/Principal/VC prior to the use, purchase or download of such software.

2.2.2 Purchase of software

The requirement of software by the user department/user is requisitioned along with specification and estimate submitted for administrative sanction to procure competitive quotations from difference suppliers for approval from Central Purchase Committee (CPC) prior to the use, purchase or installation of any such software.

All purchased software must be purchased from reputable software sellers upon approval from CPC. All purchases of software must be supported by appropriate warranty requirements and be compatible with the institution's server and/or hardware system. Any changes from the above requirements must be authorized by CPC. After the software is purchased it remains the

property of the institution and must be recorded on the software register/Stock Register/Entry book by the concerned authority like Heads of the Departments/Directors of research Center/Lab incharges/Director-Computer Center.

2.2.3 Obtaining open source or freeware software

Open source or freeware software can be obtained without payment and usually downloaded directly from the internet. All open source or freeware must be compatible with the institution's hardware and software systems.
Any change from the above requirements must be authorized by CPC.

2.2.4 Software Licensing

All computer software copyrights and terms of all software licenses will be followed by all employees of the institution. Where licensing states limited usage (i.e. number of computers or users etc.), then it is the responsibility of the Director, Computer Center/Designated faculty to ensure these terms are followed.

Andhra University, Computer Center is responsible for completing a software audit of all hardware and software annually to ensure that software copyrights and license agreements are adhered to.

2.2.5 Software Installation

All software used in Andhra University and its Constituent colleges should reflect the registered ownership of Andhra University. All software obtained in accordance with the getting software policy is to be installed on the institution's computers. All software installation is to be carried out by technical assistants or technical employees of Computer Center or with the help of authorized employees of the vendor. A software upgrade shall not be

installed on a computer that does not already have a copy of the original version of the software loaded on it.

2.2.6 Software Usage

Only software purchased in accordance with the getting software policy is to be used within the institution. Prior to the use of any software, the employee must receive instructions on any licensing agreements relating to the software, including any restrictions on use of the software.

All employees must receive training for all new software. This includes new employees to be trained to use existing software appropriately. This will be the responsibility of the concerned department Heads/ Director- Computer Center/ Registrar.

Employees are prohibited from bringing software from home and loading it onto the institution's computer hardware any unauthorized software is prohibited from being used in the institution. Any unauthorized act like duplicating of software, acquiring or use of software copies by any employee within the institution is liable for any disciplinary action by the University authorities.

2.3 Policy for Identifying USERS and their responsibilities

Policy number: AU/ITPP/P3/V1.0

USERS:

University network user community needs to observe certain precautions while getting their computers or peripherals installed so that he/she may face minimum inconvenience due to interruption of services due to hardware failures.

A. Who is Primary User?

An individual in whose room the computer is installed and is primarily used by him/her is considered to be “primary” user. If a computer has multiple users, none of whom are considered the "primary" user, the department Head should make an arrangement and make a person responsible for compliance.

B. What are End User Computer Systems

Apart from the client PCs used by the users, the university will consider servers not directly administered by Andhra University Computer Center (AUCC), as end-user computers. If no primary user can be identified, the department must assume the responsibilities identified for end-users. Computer systems, if any, that are acting as servers which provide services to other users on the Intranet/Internet though registered with the AUCC, are still considered under this policy as "end- users" computers.

C. Warranty& Annual Maintenance Contract

Computers purchased by any Section/Department/Project should preferably be with 3-year on- site comprehensive warranty. After the expiry of warranty, computers should be under annual maintenance contract. Such maintenance should include OS re-installation and checking virus related problems also.

D. Power Connection to Computers and Peripherals

All the computers and peripherals should be connected to the electrical point strictly through UPS. Power supply to the UPS should never be switched off, as continuous power supply to UPS is required for battery recharging. Further, these UPS systems should be connected to the electrical points that are provided with proper earthling and have properly laid electrical wiring.

E. Network Cable Connection

While connecting the computer to the network, the connecting network cable should be away from any electrical/electronic equipment, as they interfere with the network communication. Further, no other electrical/electronic equipment should be shared with the power supply from where the computer and its peripherals are connected.

F. File and Print Sharing Facilities

File and print sharing facilities on the computer over the network should be installed only when it is absolutely required. When files are shared through network, they should be protected with password and also with read only access rule.

G. Shifting Computer from One Location to another

Computer system may be moved from one location to another with prior written intimation to the AUCC/Head of the Department/Lab in-charge, as AUCC maintains a record of computer identification names and corresponding IP address. Such computer identification names follow the convention that it comprises building name abbreviation and room numbers. As and when any deviation from the list maintained by AUCC is found for any computer system, network connection would be disabled and same will be informed to the user by email/phone, if the user is identified. When the end user meets the compliance and informs AUCC in writing/by email or through proper channel, connection will be restored.

H. Maintenance of Computer Systems provided by the University

For all the computers that were purchased by the university centrally and distributed by the AU COMPUTER CENTER, the technical employees of

AUCC will attend the complaints related to any maintenance related problems.

I. Noncompliance

Andhra University faculty, staff, and students not complying with this computer hardware installation policy may leave themselves and others at risk of network related problems which could result in damaged or lost files, inoperable computer resulting in loss of productivity. An individual's non-compliant computer can have significant, adverse affects on other individuals, groups, departments, or even whole university. Hence it is critical to bring all computers into compliance as soon as they are recognized not to be.

J. ANDHRA UNIVERITY COMPUTER CENTER

Andhra University is having a structured strategic plan to strengthen the computerization and networking of administration. The vision of the Computer Centre is to provide complete, latest and cost-effective solution to all IT enabled activities in the University.

AUCC upon finding a non-compliant computer affecting the network, will notify the individual responsible for the system and ask that it be brought into compliance. Such notification will be done via email/telephone and a copy of the notification will be sent to the concerned authorities, if applicable. The individual user will follow-up the notification to be certain that his/her computer gains necessary compliance. The AUCC will provide guidance as needed for the individual to gain compliance.

2.4 Bring Your Own Device Policy

Policy Number: AU/**ITPP/P4/V1.0**

Purpose of the Policy

This policy provides guidelines for the use of personally owned notebooks, smart phones, tablets and other types of mobile/smart devices for institution purposes. All staff that use or access Andhra University's technology equipment and/or services are bound by the conditions of this Policy

Procedure:

At Andhra University we acknowledge the importance of mobile technologies in improving institution communication and productivity. In addition to the increased use of mobile devices, staff members have requested the option of connecting their own mobile devices to Andhra University's network and equipment.

- All devices which adhere to Governments policy like any branded/popular company's notebooks, smart phones, tablets, removable media, iphone, ipadsetc can be used.

2.4.1 Registration of personal mobile devices for institution use:

Employees when using personal devices for institution use will register and record the device with AUCC or concerned authorities. Each employee who utilizes personal mobile devices agrees:

- Not to download or transfer institution or personal sensitive information to the device. Sensitive information includes any confidential/sensitive information related to the institution, intellectual property and employee details etc.

- Not to use the registered mobile device as the sole repository for Andhra University's information. All institution information stored on mobile devices should be backed up.
- To make every reasonable effort to ensure that Andhra University's information is not compromised through the use of mobile equipment in a public place. Screens displaying sensitive or critical information should not be seen by unauthorized persons and all registered devices should be password protected.
- To maintain the device with all maintenance requirements of mobile devices such as current operating software, current security software etc and update the device software as and when required.
- Not to share the device with other individuals to protect the institution data access through the device.
- To abide by Andhra University's internet policy for appropriate use and access of internet sites etc.
- To notify the concerned authorities of Andhra University immediately in the event of loss or theft of the registered device.
- Not to connect USB memory sticks from an un trusted or unknown source to Andhra University's equipment.

All employees who have a registered personal mobile device for institution use acknowledge that the institution:

- Owns all intellectual property created on the device
- Can access all data held on the device, including personal data
- Will regularly back-up data held on the device
- Will delete all data held on the device in the event of loss or theft of the device

- Has first right to buy the device where the employee wants to sell the device
- Will delete all data held on the device upon termination of the employee. The terminated employee can request personal data be reinstated from back up data
- Has the right to deregister the device for institution use at anytime.

2.4.2 Breach of this policy

Any breach of this policy will be referred to the Vice Chancellor who will review the breach and determine adequate consequences, which can include consequences such as confiscation of the device and or termination of employee.

2.4.3 Indemnity

Andhra University bears no responsibility whatsoever for any legal action threatened or started due to conduct and activities of staff in accessing or using these resources or facilities. All staff indemnifies Andhra University against any and all damages, costs and expenses suffered by Andhra University arising out of any unlawful or improper conduct and activity, and in respect of any action, settlement or compromise, or any statutory infringement. Legal prosecution following a breach of these conditions may result independently from any action by Andhra University.

3. Information Technology Security Policy

Policy Number: AU/**ITPP/P5/V1.0**

Purpose of the Policy

This policy provides guidelines for the protection and use of information technology assets and resources within the institution to ensure integrity, confidentiality and availability of data and assets.

Procedures

3.1 Physical Security

For all servers, mainframes and other network assets under the purview of AUCC/departments/offices/hostels, the area must be secured with adequate ventilation and appropriate access through relevant security measure keypad, lock, biometric authentication etc.

It will be the responsibility of the concerned authorities to ensure that this requirement is followed at all times. Any employee becoming aware of a breach to this security requirement is obliged to notify the concerned authorities immediately.

All security and safety of all portable technology such as laptop, notepads, iPad etc. will be the responsibility of the employee who has been issued with the device such as laptop, notepads, iPads, mobile phones etc. Each employee is required to use appropriate security measures such as locks, passwords, etc. and to ensure the asset is kept safely at all times to protect the security of the asset issued to them.

In the event of loss or damage, the concerned authority will assess the security measures undertaken to determine if the employee will be required to reimburse the institution for the loss or damage. All devices such as Desktops, laptop, notepads, iPads, printers, scanners etc. when kept at the

office desk is to be secured by relevant security measure such as keypad, lock etc. provided by the authorities by the concerned staff.

3.2 Information Security

All the required important data, sensitive, valuable, or critical institution data or is to be backed-up. It is the responsibility of the concerned authorities to ensure that data back-ups are conducted frequently (Twice in a week/Daily basis) and the backed up data is kept securely in cloud, offsite venue, concerned office desk or with the concerned authority.

All technology that has internet access must have anti-virus software installed. It is the responsibility of concerned authorities to install all anti-virus software and ensure that this software remains up to date on all technology used by the institution.

All information used within the institution is to adhere to the privacy laws and the institution's confidentiality requirements. Any employee breaching this will be liable for disciplinary action by the authorities.

3.3Technology Access

Every employee will be issued with a unique identification code to access the institution technology and will be required to set a password for access as and when required.

Each password is to be set as per the prevailing guidelines and is not to be shared with any employee within the institution.

The office of Director-AUCC/concerned authorities is responsible for the issuing of the identification code and initial password for all employees.

Where an employee forgets the password or is 'locked out' after unsuccessful attempts then Director-AUCC/concerned authorities is authorized to reissue a new initial password that will be required to be changed when the employee logs in using the new initial password.

Employees are only authorized to use institution computers for personal use such as internet usage and for institutions work etc.

The following table provides the authorization of access:

S.No	Technology – Hardware/ Software	Persons authorized for access
1	Main Server Room	Director-Computer Center
2	Wi-Fi Routers, Network switch maintenance, installation of CC TV, Biometric devices	Network Engineer, software engineer
3	Campus network maintenance	Network Engineer
4	Website maintenance	Software Engineer
5	Addressing of any issue related to hardware and software	Network Engineer and software Engineer

4. Information Technology Administration Policy

Policy Number: **AU/ITPP/P6/V1.0**

Purpose of the Policy

This policy provides guidelines for the administration of information technology assets and resources within the institution.

Procedures

All the purchased software installed and the license information must be registered in the stock register/File. It is the responsibility of head of the office to ensure that this registered information is maintained. The register must record the following information:

- What software is installed on every machine

- What license agreements are in place for each software package
- Renewal dates if applicable.

The concerned authorities are responsible for the maintenance and management of all service agreements for the institution technology. Any service requirements must first be approved by CPC.

An audit is to be conducted annually by the Director, Computer center/concerned authorities to ensure that all information technology policies are being adhered to. Any unspecified technology administration requirements should be directed to Director, Computer center/concerned authorities.

4.1 Website Policy

Policy Number: **AU/ITPP/P7/V1.0**

Purpose of the Policy

This policy provides guidelines for the maintenance of all relevant technology issues related to the institution website.

Procedures

4.2 Website Register

The office of AUCC should maintain a website register which must record the following details:

- List of domain names registered to the institution
- Dates of renewal for domain names
- List of hosting service providers
- Expiry dates of hosting

The keeping the register up to date, any renewal of items listed in the register, will be the responsibility of the Director, Computer Center

4.3 Website Content

All content on the institution website is to be accurate, appropriate and current. This will be the responsibility of the Director, Computer Center or any authorized person if any appointed by AU authorities to maintain website only.

The content of the website is to be reviewed daily or as and when need arises.

The following persons are authorized to make changes to the institution website:

Director, Computer Center or any technical employee of AUCC upon the direction of the Director, Computer center

Basic branding guidelines must be followed on websites to ensure a consistent and cohesive image for the institution. All data collected from the website is to adhere to the Privacy Act.

5. Electronic Transactions Policy

Policy Number: **AU/ITPP/P8/V1.0**

Purpose of the Policy

This policy provides guidelines for all electronic transactions undertaken on behalf of the institution.

The objective of this policy is to ensure that use of electronic funds transfers and receipts are started, carried out, and approved in a secure manner.

Procedures

5.1 Electronic Funds Transfer (EFT)

It is the policy of Andhra University that all payments and receipts should be made by EFT where appropriate.

All EFT arrangements, including receipts and payments must be submitted to the concerned authorities e.g. finance department.

EFT payments must be appropriately recorded in line and must have the appropriate authorization for payment in line with the financial transactions policy of Andhra University.

EFT payments can only be released for payment once pending payments have been authorized by concerned authorities.

For good control over EFT payments, ensure that the persons authorizing the payments and making the payment are not the same person.

All EFT receipts must be reconciled to customer records once a week or as and when required.

Where EFT receipt cannot be allocated to customer account, it is responsibility of the concerned authority to investigate. In the event that the customer account cannot be identified within 15 days or one month, the concerned authority must take appropriate action for the receipted amount.

It is the responsibility of concerned authority/Finance officer to annually review EFT authorizations for initial entry, alterations, or deletion of EFT records, including supplier payment records and customer receipt records

5.2 Electronic Purchases

All electronic purchases by any authorized employee must adhere to the purchasing policy of Andhra University.

Where an electronic purchase is being considered, the person authorizing this transaction must ensure that the internet sales site is secure and safe and be able to demonstrate that this has been reviewed.

All electronic purchases must be undertaken under the authorization and supervision of the concerned authorities adhering to the financial policies of Andhra University.

5.3 IT Service Agreements Policy

Policy Number: **AU/ITPP/P9/V1.0**

Purpose of the Policy

This policy provides guidelines for all IT service agreements entered into on behalf of the institution.

Procedures

The following IT service agreements can be entered into on behalf of Andhra University

- Provision of general IT services
- Provision of network hardware and software
- Repairs and maintenance of IT equipment
- Provision of institution software
- Provision of mobile phones, servers, laptops, smart devices, biometric devices etc and relevant plans
- Website design, maintenance etc.

- Cloud services

All IT service agreements must be reviewed by Director - Computer Center, University recommended lawyer before the agreement is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Vice Chancellor.
All IT service agreements, obligations and renewals must be recorded and maintained in Register office or the office of concerned authorities.

Where an IT service agreement renewal is required, in the event that the agreement is substantially unchanged from the previous agreement, then this agreement renewal can be authorized by Registrar of the University.
Where an IT service agreement renewal is required, in the event that the agreement has substantially changed from the previous agreement, the concerned authorities must review before the renewal is entered into. Once the agreement has been reviewed and recommendation for execution received, then the agreement must be approved by Vice Chancellor.

In the event that there is a dispute to the provision of IT services covered by an IT service agreement, it must be referred to Registrar/Vice Chancellor who will be responsible for the settlement of such dispute.

6. Emergency Management of Information Technology

Policy Number: **AU/ITPP/P10/V1.0**

Purpose of the Policy

This policy provides guidelines for emergency management of all information technology within the institution.

Procedures

6.1 IT Hardware Failure

Where there is failure of any of the institution's hardware, this must be referred to Director-Computer Center/concerned authorities immediately.

It is the responsibility of Director-Computer Center/concerned authorities to look into the issue and analyze the causes in the event of IT hardware failure.

It is the responsibility of Director-Computer Center/concerned authorities to undertake tests on planned emergency procedures half yearly to ensure that all planned emergency procedures are appropriate and minimize disruption to institution operations.

6.2 Point of Sale Disruptions

In the event that point of sale (POS) system is disrupted, the following actions must be immediately undertaken:

- POS provider to be notified
- Concerned authorities must be notified immediately
- All POS transactions to be taken using the manual machine located below the counter.
- For all manual POS transactions, customer signatures must be verified
- Any other appropriate and relevant action needed.

6.3 Virus or other security breach

In the event that the institution's information technology is compromised by software virus or any possible security breaches, such breaches are to be reported to Registrar/ Vice Chancellor immediately.

Director-Computer Center is responsible for ensuring that any security breach is dealt with within one day to minimize disruption to institution operations.

6.4 Website Disruption

In the event that institution website is disrupted, the following actions must be immediately undertaken:

- Website host to be notified
- Registrar, Vice Chancellor must be notified immediately
- Technical team of AUCC should immediately respond to the emergency and take necessary actions on the direction of University authorities.

7. Video Surveillance Policy

Policy Number: **AU/ITPP/P10/V1.0**

The system or CCTV comprises of

- Fixed position cameras; Pan Tilt and Zoom cameras; Monitors: Multiplexers; digital recorders; SAN/NAS Storage; Public information signs.
- Cameras will be located at strategic points on the campus, principally at the entrance and exit point of sites and buildings. No camera will be hidden from view and all will be prevented from focusing on the frontages or rear areas of private accommodation.
- Signs will be prominently placed at strategic points and at entrance and exit points of the campus to inform staff, students, visitors and members of the public that a CCTV installation is in use.
- Although every effort has been made to ensure maximum effectiveness of the system it is not possible to guarantee that the system will detect every incident taking place within the area of coverage.

Purpose of the system

The system has been installed by university with the primary purpose of reducing the threat of crime generally, protecting universities premises and helping to ensure the safety of all staff, students and visitors consistent with respect for the individuals' privacy. These purposes will be achieved by monitoring the system to:

- Deter those having criminal intent
- Assist in the prevention and detection of crime
- Facilitate the identification, apprehension and prosecution of offenders in relation to crime and public order
- Facilitate the identification of any activities/event which might warrant disciplinary proceedings being taken against staff or students and assist in providing evidence to managers and/or to a member of staff or student against whom disciplinary or other action is, or is threatened to be taken.
- In the case of security staff to provide management information relating to employee compliance with contracts of employment

The system will not be used:

- To provide recorded images for the world-wide-web.
- To record sound other than in accordance with the policy on covert recording.
- For any automated decision taking.

7.1 The Security Control Room

- Images captured by the system will be monitored and recorded in the Andhra University Computer Center Security Control Room, "AUCC control room", twenty-four hours a day throughout the whole year.

Monitors are not visible from outside the control room.

- No unauthorized access to the AUCC control room will be permitted at any time. Access will be strictly limited to the duty controllers, authorized members of senior management, police officers and any other person with statutory powers of entry.
- Staff, students and visitors may be granted access to the AUCC control room on a case-by-case basis and only then on written authorization from the Registrar. In an emergency and where it is not reasonably practicable to secure prior authorization, access may be granted to persons with a legitimate reason to enter the AUCC control room.

- Before allowing access to the AUCC control room, staff will satisfy themselves of the identity of any visitor and that the visitor has appropriate authorization. All visitors will be required to complete and sign the visitors' log, which shall include details of their name, their department or organization they represent, the person who granted authorization and the times of entry to and exit from the centre. A similar log will be kept of the staff on duty in the AUCC control room and any visitors granted emergency access.

7.2 AU Security Control Room Administration and Procedures

- Details of the administrative procedures which apply to the AU Control Room will be set out in a Procedures Manual, a copy of which is available for inspection by prior arrangement, stating the reasons for the request.
- Images of identifiable living individuals are subject to the provisions of

the Prevailing Data Protection Act; the AUCC Control Room Supervisor is responsible for ensuring day to day compliance with the Act. All recordings will be handled in strict accordance with this policy and the procedures set out in the Procedures Manual.

7.3 AU Security Control Room Staff

All staff working in the AUCC Control Room will be made aware of the sensitivity of handling CCTV images and recordings. The AUCC Control Room Supervisor will ensure that all staff are fully briefed and trained in respect of the functions, operational and administrative, arising from the use of CCTV.

7.4 Recording

- Digital recordings are made using digital video recorders operating in time lapse mode. Incidents may be recorded in real time.
- Images will normally be retained for fifteen days or as per the company specifications of the recorder from the date of recording and then automatically over written and the Log updated accordingly. Once a hard drive has reached the end of its use it will be erased prior to disposal and the Log will be updated accordingly.
- All hard drives and recorders shall remain the property of university until disposal and destruction.

7.5 Access to images

- All access to images will be recorded in the Access Log as specified in the Procedures Manual
- Access to images will be restricted to those staff need to have access in accordance with the purposes of the system.

- Disclosure of recorded material will only be made to third parties in strict accordance with the purposes of the system and is limited to the following authorities:
- Law enforcement agencies where images recorded would assist in a criminal enquiry and/or the prevention of terrorism and disorder
- Prosecution agencies
- Relevant legal representatives
- The media where the assistance of the general public is required in the identification of a victim of crime or the identification of a perpetrator of a crime
- People whose images have been recorded and retained unless disclosure to the individual would prejudice criminal enquiries or criminal proceedings.
- Emergency services in connection with the investigation of an accident.
- Upon the instruction of AU higher authorities.

7.6 Complaints

- It is recognized that members of University and others may have concerns or complaints about the operation of the system. Any complaint should be addressed in the first instant to the AUCC Security Control Room in-charge or the Director-Computer Center. Concerns or enquiries relating to the provisions of the prevailing Data Protection Act may be addressed to the Data Protection Officer, These rights do not alter the existing rights of members of University or others under any relevant grievance or disciplinary procedures.
- The contact point for members of University or members of the public wishing to enquire about the system will be the AUCC Security Office/

Director-Computer Center which will be available during the working hours of the University except when University is officially closed.

- Upon request enquirers will be provided with:

(i) A summary of this statement of policy
(ii) An access request form if required or requested
(iii) A subject access request form if required or requested
(iv) A copy of the University central complaints procedures

- All documented procedures will be kept under review and a report periodically made to the Management Representative Committee/AU authorities.

REGISTRAR
ANDHRA UNIVERSITY
VISAKHAPATNAM-530 003

ANDHRA UNIVERSITY
WALTAIR

Prof. D. LALITHA BHASKARI
Coordinator IQAC & ISO
Andhra University
Visakhapatnam-530 003

Appendix - I

Andhra University Computer Center (AUCC)

Andhra University is having a structured strategic plan to strengthen the computerization and networking of administration. The vision of the computer centre is to provide complete, latest and cost-effective solution to all IT enabled activities in the University. The Campus network bandwidth 100Mbps is upgraded to 1 Gigabit Backbone Connectivity with a view to provide secured administrative computing services to facilitate teaching and administrative tasks. As a precautionary measure, it is equipped with BSNL Network bandwidth of 200mbps to the university for meeting the unexpected failures.

There is an extensive effort to provide a central computing facility with Network Server for all the students as well as staff of the University to provide Internet and Wifi facility. The bandwidth is sufficiently raised for the departments and the Computer Centre wherever necessary. A consolidated network will definitely improve the performance of the Internet accessibility across the University constituent colleges.

The Computer Centre, AU has developed a software portal to pay the tuition fee through online, which facilitates the students of all University Constituent Colleges for paying the fee from their residences. Whenever the results are announced, the students are to be provided the information (SMS) through their registered mobiles, which facilitates them not to wait for receiving the marks statements.

The University has installed the surveillance cameras in the departments, students' hostels and some sections to monitor and assess the functioning of the respective offices. The online Aadhar-based attendance is being taken from the

faculty and non-teaching staff and also is extending the same to the campus students.

Being large campus network maintaining secure network, the computer centre has installed an antivirus (kaspersky) for 500 users. The entire admission process is computerized and admissions are carried through on-line counseling. The CAO is provided with Wi-Fi facility and with Cisco UCS chassis 5108 with two Cisco blade servers with fabric interconnect, EMC storage of 6TB with secure remote control gateway clients. Official emails about 25,000 are provided to the Administrators/Principals/Deans/Directors/Coordinators/ faculty/scholars.

Both wired and wireless LAN is available. Whole campus network is on optical fibre. For wireless connectivity the campus has Cisco 2504 wireless controller with 50 AP licenses, Cisco catalyst 4500 E-series switch with controlling licensed software, catalyst 2960S 24 GigE, fXSFP LAN Base, Cisco catalyst 3560X24 port data LAN Base.

All most all the class rooms are equipped with electronic team boards, audio, internet and other equipment used for interactive sessions and the proceedings can be recorded. Most of these rooms can accommodate about 50 to 200 members.

The University has equipped about 15 Digital Class rooms in Andhra University College of Engineering for benefitting the students. It helps the student community for training towards digitalization to compete with other Higher Learning Institutions. Steps have been taken for extending of 40 more E-class rooms from this academic year.

The computer center has taken up a project for introduction of automation in the Accounts Wing. It facilitates the day-to-day remittances and transactions of the university as well as the receipts from the various affiliated colleges.

To achieve the goals of E-governance, the university is planning to introduce the e-filing, file-tracking system, etc. It facilitates to pave the way to give solutions and make decisions for speedy administration on the part of the University.

In coming five years, to synchronize all the activities in the areas like administration, admissions, research, teaching, placement schedules, cultural events, sports, publication of results, it has a view to strengthen the administration digitally and give strong support for its end-users.

The university has a surveillance system which covers all the important places. It will be extended to fix up at least 250 cctv cameras in and around the campus for monitoring and recording the footage in the University server.

The Computer centre has installed 84 Biometric devices for teaching and non-teaching staff for taking daily attendance, all these biometric devices are connected to NIC. It has further planned to install 350 biometric devices for students and research scholars for taking attendance under RUSA funds.

Facilities & Services

The campus wide area network is for connecting the various departments /admin buildings. The core backbone employs single mode optical fiber connecting various departments. At certain places multi-mode fiber optic cable was used. At present the campus wide networking, IT service support and software development is being executed by Andhra University Computer Centre.

AUCC provides the following facilities and services:

I. www.andhrauniversity.edu.in mail services in Google cloud

II. www.aucoe.info web site maintenance

III. Anti-virus updates/installation in campus colleges

IV. Network maintenance

V. Internet connectivity and bandwidth, maintenance

VI. Network security and authentication services

VII. Student information/data maintenance

VIII. Pre and post exam data processing

IX. DD Cell computerization

X. Pensioners Pay slips online

AUCC is in the process of expanding its activities to provide assured unlimited campus connectivity to every nook and corner of the University. Over the last one year an enormous growth in network usage was observed in the campus with various changes and configurations in the critical parts of the network. Partially a few hostels were extended with wired and wireless network connectivity in addition to computers.

They are three wings which computer centre mainly consists of

1.Software wing for application development

2.Network Wing for network deployment and maintenance

3.Data wing for data management

Roles and responsibilities of Software wing:

- Deploying Web Solutions towards Student exam registration, online student portal applying original degree, provisional certificates, duplicate records of certificates

- Transaction management Towards fee Payment for different purposes in and out for the university
- Online Result management for students
- Chat Bot Maintenance towards enquires of the students
- Faculty Profile Management for faculty members to keep their profile updated
- Online Feedback system for students to give their feedback on their faculty with transparency
- Salary Management system for SII section to generate salaries and access for faculty members to check their salaries
- Periodic maintenance and updating the domain websites www.andhrauniversity.edu.in, www.aucoe.in
- Result processing for all UG & PG Courses Present in the university . University in total has 328 courses in all the modes together
- Issue of all original degree , provisional certificates, consolidated mark sheets for all UG & PG Courses in the university and affiliated colleges of university.

No of staff Working for Software wing : 7 members

Infrastructure in the wing:

Physical Server - 2 No with the below configuration:

HP M-350 G6 SERVER WITH INTEL XEON QUAD CORE PROCESSOR E5540 / 6BG DDR3 ECC PC-10600 MEMEORY / 2x300 GB SAS HARD DISK DRIVES

15K/ INTEL SERVER CHIPSET / INTEGRATED P410i SATA /SAS CONTROLLER

With 2 virtual Machines and 2 Vspheres

Cloud Infrastructure:

Microsoft Entrepreneur Account Access for using 4 virtual machines and 2 relational databases

With 32GB RAM, 4TB STORAGE for all profiles

Workstations:

10 workstations HPG30 with i3 processors ,8GB RAM and 1TB hard disk

Network Wing Roles and Responsibilities:

- Installing and Configuring Cisco Layer2 & Layer3 Switches and Inter VLAN Management.
- Monitoring of all Links (LAN, WAN & WLC).
- Taking IOS Backup's of Firewalls, Routers & Switches.
- POINT-to -POINT Configuration like (UBIQUTI, CAMBIUM).
- Responsible for Monitoring all Optical Fiber links in Network (Single Mode & Multi Mode).
- Implementation of TCP/IP, DHCP, DNS, TFTP, FTP, SNMP, Active Directory Services and Linux
- Platform under various LAN/WAN environments.
- Experience with Virtualization technologies like Installing, Configuring and administering VMware
- ESX/ESXi and created and managed VMs (virtual server) and also involved in the maintenance of the
- virtual server.
- Designed, configured and implemented a Cisco UCS B200 M3 Blade server with EMC Storage
- Connectivity with Fabric 10G Switches.

- Troubleshooting LAN Connectivity Problems and Internet Problems such as Shared level problems,
- Unidentified Network Problem, Cable problems.
- Extending support to the network infrastructure and Maintaining LAN including hubs, Switches, Modems, Network cables etc...,
- Configured and Managed Cisco Wireless Access Points and Cisco Wireless LAN Controllers (WLC) through Cisco Wireless Control System (WCS).
- Installing and Configuring Ruckus Access points with respective to Ruckus Zone Directors to
- implement Wi-Fi in University Hostels.
- Maintained and supported the network infrastructure of the organization which consists of over 1500
- live users.
- Installing and Configuring Bio-Metric devices (AADHAR Linked) for access control of the students and employees.
- Identifying and resolving configuration issues understanding and logical approach to fault finding in
- network.
- Development and Maintaining Cisco Devices Network Infrastructure in Andhra University Data Centre.
- Maintenance of NVR's, Cameras.

Infrastructure for Network WING

Firewall Details :

Model: Cisco ASA 5545 Firewall

Cisco Core Switch:

Cisco Catalyst 6807

Switches:

Cisco 3560

Cisco 2960

Cisco SG300

Cisco SG350

Cisco 3560 PoE Switches

Dlink Websmart Switches

Wireless Controllers:

Cisco Wireless controller

Total no of Accesspoints: 75

Ruckus Zone director 1200 Series

Total no of Accesspoints :44

Ruckus zone Director 3000 Series

Total no of Accesspoints : 125

Cyberoam Details:-

Cyberoam CR500iNG

Cyberoam CR35iNG

Biometrics:

Total no of Biometric Devices installed in campus is 330 devices.

Camera Details:

Total no of Cameras installed in campus is 226 Cameras

Internet users and clients:

Wifi Users :5700

Wired Users: 3800

The whole campus connected with fibre connectivity -15,000mtrs (Both Single

mode and Multimode)

Employees Working for network wing: 7

Workstations:

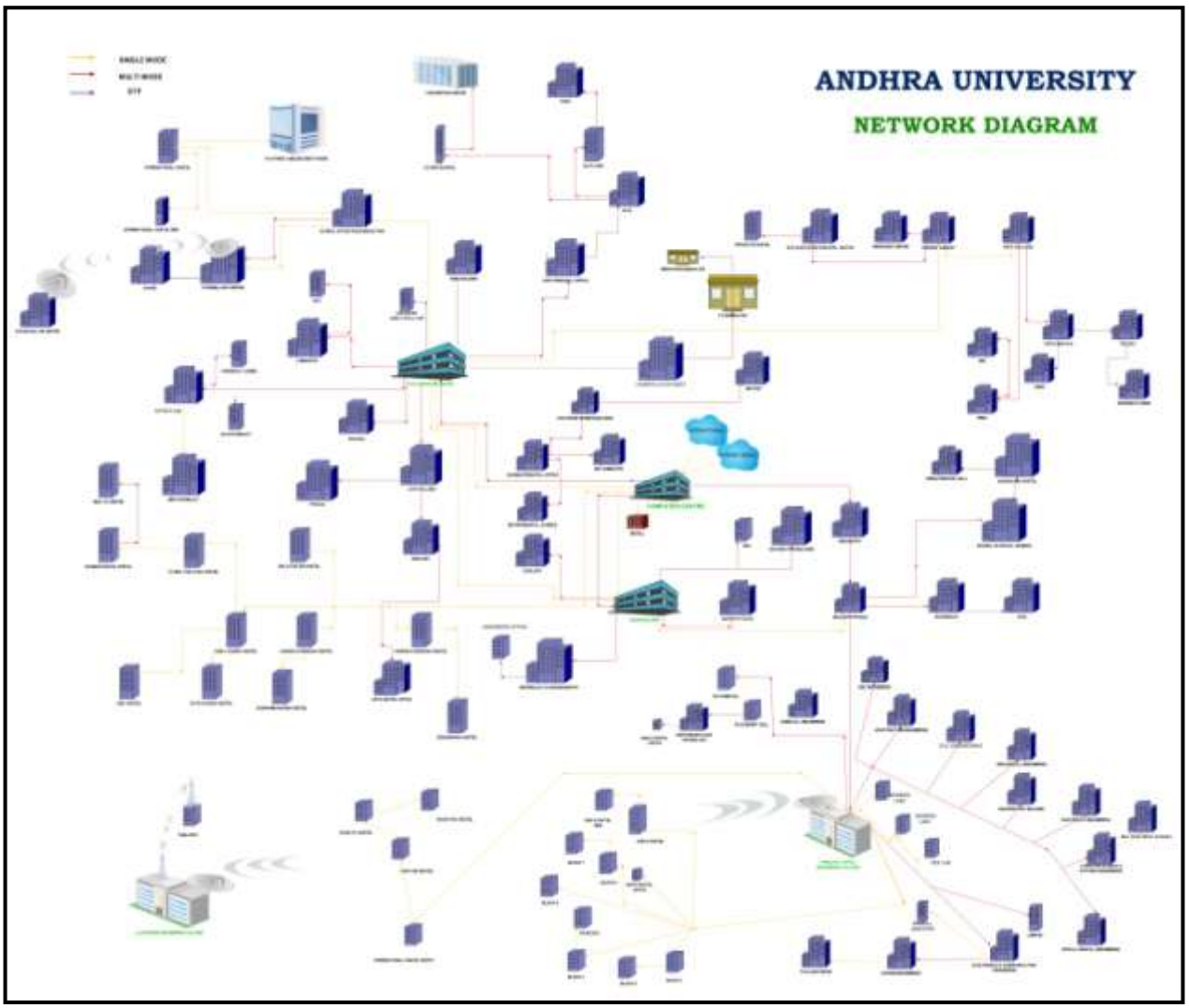
15 workstations HPG30 with i3 processors ,8GB RAM and 1TB hard disk

Roles and responsibilities of Data Wing

To Support network and software engineers for data essentials

To support data input for results processing

45 workstations HPG30 with i3 processors ,8GB RAM and 1TB hard disk



AU Network Diagram