Information Technology (IT) Policy

1. Policy statement

1 Kakatiya University, Warangal views Information Technology (IT) as the medium for ensuring optimum dissemination of knowledge through its academic, non-academic pursuits and administrative service to all the stakeholders for the criterion of a knowledge society by molding the builders of future.

2 IT policy exists to create, maintain, secure, and ensure legal and appropriate use of Information technology infrastructure established in the college campus. This policy establishes Institution-wide strategies and responsibilities for protecting the **C**onfidentiality, **I**ntegrity, and **A**vailability of the information assets that are accessed, created, managed, and/or controlled by the college. Information assets addressed by the policy include data, information systems, computers, network devices, intellectual property, as well as documents and verbally communicated information.

3 IT security involves the protection of information assets from accidental or intentional disclosure, modification, or denial at a reasonable cost.

4 University Campus Networking Lab (UCNL) at Kakatiya University aims at identifying, providing and maintaining reliable computing facilities, computing network environment, communication facilities and related infrastructure to facilitate education and research.

2. Objectives

1 UCNL reserves the right to monitor the usage of the facilities provided therein to maintaina secure computing environment and to abide by the legal norms that exist.

2 In this document, the term “users” shall mean individuals, staff, students, faculty, departments, offices or any other entity which fall under Kakatiya University Campus and require anyservices aforesaid.

3 Users are bound by all the rules and regulations formulated by the Institution from time to time on use of computing facilities provided to them or owned by them.

4 This document is meant for internal circulation and all users shall have access to this document.

I **Acceptable IT Devices**

1 Any computer, peripheral or network capable device connected to campus network must belong to, or be formally registered, or be hosted by UCNL.

2 UCNL reserves the right to restrict access otherwise.

II Responsibilities of users and user groups

1 All users shall comply to existing federal, state and, other applicable laws. Following copyright laws regarding protected commercial software or intellectual property.

2 Abiding government, telecommunications and networking laws and regulations.

3 Honouring acceptable computer use policy of computer networks accessed through campus network either locally or remotely.

4 Sensitive to resource utilization and help to provide fair distribution of computer resources by minimizing unnecessary network traffic that may interfere with the ability of others to make effective use of campus network resources.

III Data network responsibilities of end users

1 Individual department, users or user groups may develop their own local area networks or local communications environment within, only if those facilities are approved by UCNL and meets developed network standards. UCNL shall also reserve the rights to monitor such networks.

2 Any user group or department intending to establish connectivity to external data communications network directly should do so after coordinating with UCNL. UCNL shall extend all necessary technical support to user groups or departments who intend to establish such connections to external data communications. All such direct communication networks shall be routed physically or logically through the central network operations center of UCNL to maintain security to the campus network.

IV Computing facility provisioning and maintenance

1 UCNL is responsible for provision and maintenance of computing facilities providedto users. The facilities are provided after the user secure approvals from the management.

2 The user shall ensure physical safety of the equipment and produce the same as and when required for stock verification by UCNL. If any peripheral or components of the equipment assigned is found missing, the user shall report the same to UCNL forfurther action.

3 The user shall obtain prior approval from UCNL before plugging in any additional peripherals to the local area network (LAN). This is also applicable to connect peripherals to external ports like USB, RS232, IEEE1394 etc.

4 UCNL shall not be responsible for any failure to personal peripherals connected to

institute equipment by the user.

5 Users shall ensure data availability and security by taking regular backups of the data stored on their systems.

6 The individual or the department shall be responsible to report any hardware or software related faults to UCNL through facilities provided for reporting. UCNL shall take all necessary steps to resolve the issue at the earliest. However, faults that require substantial additional financial expense may need to be approved by competent authorities.

7 All support calls attended by support personnel shall be documented and the user or department shall insist to get a written service report from the service personnel regarding the support offered. The individual or the department shall ensure that the service report is complete in all respect including components that have been removed or replaced by the service personnel.

8 The ownership of the equipment assigned to the individual or the department shall remain with the College.

9 Possession of computing equipment's by students within the campus shall be governed by the rules and regulations formulated by the College separately. However, students shall be bound by all the provisions of the IT policy with respect to the usage of such equipment with the campus.

V Provision of computing software and maintenance

1 UCNL shall provide all necessary software for operating the devices allocated to the user.

2 UCNL reserves the right to secure the administrative passwords for all the devices owned by the Institute.

3 Users may install any software on the equipment allotted to them after obtaining prior approval from UCNL . All such software that may be installed on the equipment shall be used for the purposes as mentioned in Para 1.2. However, UCNL shall reserve the right to restrict users from installing any software that may pose a risk to the security and integrity of the equipment and the campus network.

4 All software installed on the user machines shall be legal copies from the original vendors. Users are encouraged not to use any illegal or unlicensed versions of copyrighted software.

5 UCNL shall ensure reinstallation of system and application software if required. Users shall request for the same through facilities provided for making such support

requests.

6 Users shall not copy, duplicate or distribute any software owned by the College or downloaded by them to their PCs.

VI Provision of network connectivity and maintenance

1 UCNL is responsible for providing users with data communications connectivity from their building to all campus-wide network services.

2 UCNL provides data communications connectivity to allow access from a terminal,PC, accepted devices or user group to campus-wide network services for purposesmentioned in Para 1.2.

3 UCNL is responsible for the design, development, and maintenance of campus-widenetwork facilities that are used to connect all users, including facilities such as ISDN, leased data links, fiber optic backbone network or any other technologies that may be adopted.

4 UCNL will proactively monitor the shared networks to detect problems and will takeactions necessary to isolate the cause and correct the problem.

5 Personal devices of users shall be connected to the network after registering the same with the UCNL.

VII LAN and Intranet security

1 Computer networks are designed to be open systems and facilitate access to networked resources, data applications system security must rely primarily on the proper application system design and network operating system configuration, rather than on secure physical network facilities.

2 UCNL is responsible for maintaining physical security of all network equipment anddata communications cabling in campus equipment closets, between buildings andin network hub locations.

3 UCNL is responsible for the integrity of all software running on the backbone network equipment, including network control servers, communications servers, LAN switches, routers, and gateways.

4 Users are encouraged to assist UCNL in maintaining the physical security of the network assets installed at their location and to ensure the integrity of all network related services running on their local hosts.

5 UCNL shall take all necessary security measures to protect and secure the device connected to network and avoid compromises. This may include undisclosed administrator level passwords, restricted access to external or internal ports,

restriction on installation of system software by the users, etc.

6 Compromised or problem hosts connected to the network, once identified will be denied access until they are repaired.

7 To ensure network security, UCNL shall monitor all traffic on the network using appropriate software to identify malicious traffic. If malicious traffic is identified, the host that generated or generating the traffic shall be logically or physically disconnected from the network. UCNL shall recommend remedial actions for such devices connected to the network, which may include: removal of malicious software, fully patched Operating Systems; current anti-virus software and virus definitions; secure passwords, personal firewalls, intrusion detection software, etc. UCNL shall provide necessary support to users for the aforesaid actions.

8 UCNL shall also extend support to users connecting their personal devices to the campus network but limited to the operational or legal constraints.

VIII Provision of network services

1 UCNL shall host all necessary network services to support the activities of the users. This shall include internet connectivity, email services, ftp servers, DNS, DHCP, etc. The usage of the services shall be for the purposes as mentioned in Para 1.2 and shall be monitored and controlled by UCNL.

2 These services are provided for the purpose of increasing the job fulfillment, job performance, and to increase the productivity.

3 Users shall fill up necessary application forms and secure approval from competent authorities to access services hosted by UCNL.

4 Users shall not divulge passwords, software license codes or other security codes allotted to them to third party. Users are encouraged to reset their passwords every 90 days to ensure access security. All systems-level passwords (e.g., root, enable, network administrator, application administration accounts, etc.) must be changed at least every 90 days.

5 Users shall not use University network services to view, download, save, receive, orsend material related to or including:

a) Offensive content of any kind, including pornographic material

b) Promoting discrimination based on race, gender, national origin, age, marital status, sexual orientation, religion or disability.

c) Threatening or violent behavior.

d) Illegal activities.

e) Commercial messages.

f) Messages of a political or racial nature.

g) Gambling.

h) Personal financial gain.

i) Forwarding e-mail chain letters.

j) Spamming e-mail accounts from university e-mail services or computers.

k) Material protected under copyright laws.

l) Sending business-sensitive information by e-mail or over the Internet.

m) Dispersing organizational data to non- university personnel without authorization.

n) Opening files received from the Internet without performing a virus scan.

o) Recreational streaming of internet material, such as radio, video, TV, or stock tickers.

p) Downloading and/or installing programs/software on any network computer(s) without authorization from the UCNL.

q) Tampering with your university domain e-mail ID to misrepresent yourself and University to others.

6 UCNL may shutdown the network services periodically for maintenance purposes. Users shall be informed well in advance regarding such outages.

7 Information regarding such maintenance schedules shall be sent to users through available means of communication which may include but not limited to emails, instant messaging apps or hard copy circulars.

IX Network activities not permitted over the campus network

1 Execution of software programs which excessively consume network or network server resources.

2 Activities that violate rules of local administration, the State, Central Government or recognized International Organization or Treaties.

3 Activities that interfere with the legitimate function of other devices connected to campus network. (examples include DHCP Servers, devices running RIP, RAS Servers consuming DHCP Addresses which have not been registered with UCNL, etc.)

4 Configuring mail servers with open relays, sending unsolicited mails, commercial mails, spamming.

5 Downloading large files for personal use including music, video and software.

6 Probing, scanning or other activities that amount enumeration of campus network.

7 Initiating Denial of Service Attacks, Hacking, Cracking or similar activities which disrupt the network services hosted internally and externally.

8 Executing network related software for packet sniffing, content sniffing.

9 Unauthorized access to internal or external network services, devices, servers, or hosts.

10 Illegal distribution of any copyrighted material.

11 "Stealing" or "Borrowing" IP addresses.

12 Any activity that tarnishes University's professional image. (UCNL may not be the policing agency in these matters)

X Violations

1 Violations will be reviewed on a case-by-case basis.

2 If it is confirmed and proved that a user has violated one or more of the above use regulations, that user will receive a reprimand from his or her Head of the Department or reporting authority and his or her future use will be closely monitored.

3 If a gross violation has occurred, the Management will take immediate action. Such action may result in losing Internet and/or e-mail privileges, severe reprimand, and or disciplinary action.

4 During the investigation of an alleged policy violation, a user's computing and network access may be suspended.

5 The decision of the Management shall be final and binding on the constituents in case of any conflict or dispute.